coinbase

To:
The U.S. Department
of the Treasury

October 17, 2025

Re: Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets

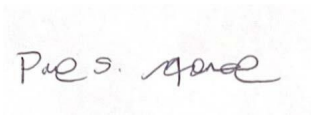
Coinbase Global, Inc. ("**Coinbase**") appreciates the opportunity to respond to the U.S. Department of the Treasury's Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets.

Coinbase is the most trusted service provider of crypto trading, custody, and infrastructure in the world. Founded in 2012 and publicly listed on the NASDAQ, we offer a secure interface for millions of verified retail and institutional investors globally. We are committed to building an open financial system and are doing so with the strongest regulatory compliance and security protocols available.

Coinbase fully supports the Administration's policy towards the responsible growth and use of digital assets, as outlined in the Executive Order 14178 on "Strengthening American Leadership in Digital Financial Technology." We also appreciate the efforts being made by the Department of the Treasury to modernize the Bank Secrecy Act through the promotion of innovative technology, techniques and methods designed to counter illicit finance in the digital asset sector.

To assist the Department of the Treasury in these efforts, Coinbase is providing the following comments that are based on our extensive experience in this space. We look forward to working with the Department of the Treasury on this initiative going forward.

Yours sincerely,



Paul Grewal
Chief Legal Officer

Coinbase

I. Executive Summary

Coinbase welcomes the U.S. Department of the Treasury's ("**Treasury**") efforts to promote new technologies in the fight against illicit financial activities through this Request for Comment ("**RFC**"). In the world of financial crime, money laundering schemes have become increasingly sophisticated, leveraging advanced technologies and global networks in an attempt to evade detection. Compounding the challenge is the sheer volume and speed of financial transactions processed daily, especially in the digital asset ecosystem.

Blockchain and other innovative technologies can counter these emerging risks. Treasury and other policymakers should promote their use to identify and deter illicit activity. Doing so would support a primary objective of the Anti-Money Laundering Act of 2020 ("**AMLA**")[1], which sought to modernize the Bank Secrecy Act ("**BSA**") by:

1) Prioritizing innovation and providing opportunities for financial institutions to enhance their compliance programs through technological innovation; and

2) Revisiting or eliminating "outdated" or "redundant" regulations through significant rulemaking changes.

While the RFC is based on a requirement under the Guiding and Establishing National Innovation for U.S. Stablecoins Act ("**GENIUS Act**"), it offers Treasury a greater opportunity to revisit AMLA's objectives and current BSA regulations that have not always promoted the use of innovative technologies to fight illicit activity.

Coinbase's main points for each of the RFC topics are as follows:

Application Programming Interfaces: Treasury should further support adoption of Application Programming Interfaces ("**API**") by issuing clear guidance that establishes safe-harbors within the BSA when financial institutions properly use APIs to satisfy their anti-money laundering and counter-terrorist financing ("**AML/CFT**") obligations. Such guidance would establish the conditions that must be met (e.g., governance, integration with other compliance systems, ongoing testing) before financial institutions can avail themselves of those safe-harbors, and these conditions should be informed by additional public-private collaboration and regulatory sandboxes.

- APIs have become an essential component in the AML/CFT and sanctions controls of financial institutions. The majority of software solutions in this field are API-based because APIs enable real-time data exchange, seamless integration

[1] Div. F of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, Div. F, 134 Stat. 3388, 4547 (2021).

with third-party tools, and the ability to scale compliance systems as transaction volumes grow. APIs allow financial institutions to connect to blockchain analytics platforms, sanctions screening databases, and transaction monitoring systems, creating a unified compliance ecosystem. This interoperability is critical in an increasingly complex compliance environment, where institutions must process vast amounts of data quickly and accurately to detect illicit activity.

- Despite their advantages, APIs face challenges such as lack of standardization, data quality issues, and regulatory fragmentation. To solve these challenges, Treasury should issue guidance that clearly defines regulatory expectations for API-driven AML compliance technologies – such as outlining acceptable use cases, data privacy requirements, and standards for interoperability – allowing firms to confidently adopt and integrate APIs into their programs. Additionally, encouraging the use of industry-standard protocols, supporting regulatory sandboxes for innovative API solutions, and clarifying the use of third-party vendors would reduce uncertainty, streamline implementation, and enhance the effectiveness of AML/CFT controls across the sector.

Artificial Intelligence: Treasury should accelerate the responsible adoption of artificial intelligence ("**AI**") by issuing regulations and guidance that provide the industry with clear parameters to follow when seeking to adopt this technology – specifically, in the form of regulatory safe-harbor within the BSA – that will encourage exploration and use of AI.

- AI is a transformative technology in the AML/CFT sector – as it is for many other sectors – that will revolutionize how financial institutions and law enforcement fight illicit activity. AI's inherent benefits include reducing false positives, enabling real-time processing at scale, and freeing up Compliance resources to focus on higher-risk activity.

- However, to date, U.S. firms have been hesitant to fully unlock AI within their AML/CTF programs given the lack of regulatory clarity as to what use-cases are permitted under applicable AML/CTF laws and regulations.

- Accordingly, we recommend that Treasury issue guidance – similar to its 2019 guidance on custodial versus non-custodial AML/CFT obligations[2] – establishing a BSA safe-harbor for regulated entities that use AI to satisfy AML/CTF and sanctions obligations, so long as certain conditions are met. Such conditions should be informed by public-private collaboration that focuses on outcomes,

[2] U.S. Dep't of the Treasury, Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001, at 15-16 (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

governance, and human oversight and encourages responsible integration of on-chain with off-chain data, rather than mandating specific models that inhibit innovation.

Digital Identification: Treasury and Congress should update the BSA's customer identification requirements and relevant guidance to include decentralized identification ("**DiD**") and zero-knowledge-proofs ("**ZK Proofs**") as part of an approved identity verification process – specifically, through amending FinCEN regulations or issuing guidance that authorizes these forms of digital identification as acceptable forms of non-documentary verification.[3] Relatedly, the legal framework for "reliance" – where one regulated entity relies on the customer due diligence performed by another – should also be amended to support the use of innovative identification techniques and allow for an interoperable identity ecosystem where a customer's verified identity can be securely and efficiently reused.

- The BSA's current requirements around verifying a customer's identity are archaic. Gone are the days when a person walks into a bank and presents identification documents to open a bank account. Most account openings today, even at traditional financial institutions, are done remotely. Requiring firms to collect copies of identification documents online, both at onboarding and on an ongoing basis, not only presents a tremendous identity theft risk but also requires immense compliance resources that could be better used elsewhere to fight illicit activity.
- Therefore, Treasury and Congress should work together to amend the BSA to: (1) clearly denote that DiDs are an acceptable form of non-documentary verification; and (2) further unlock the ability of one regulated financial institution to rely on the prior due diligence performed by another through a DiD sharing safe-harbor.

Blockchain Technology: Treasury should publish supervisory guidance that explicitly recognizes and incentivizes the use of Know Your Transaction ("**KYT**") screening and blockchain analytics clustering as a more effective means of enhancing AML/CFT compliance than is available in traditional finance. Legislation and guidance should also be updated to specifically list such technology as an example of proper, risk-based ongoing monitoring and sanctions screening.

- While various federal and state regulators have already promoted the utility of blockchain technology in the digital assets space, amendments to the BSA and more detailed regulatory guidance would further unlock this digitally native solution that makes compliance more accurate, efficient, and protective of user data across the entire financial system.

[3] *See, e.g.*, 31 C.F.R. § 1020.220(a)(2)(ii)(B)(1).

- Further legislation and regulatory guidance can actively promote the use of blockchain technology for compliance by creating a clear and supportive regulatory environment for "RegTech" innovation, such as smart contract-based controls for AML and sanctions screening. This also includes providing legal clarity for the use of AI and DiD. The updated guidance should further encourage the sharing of information relevant to potential illicit activities routed through blockchains, while being careful not to overimpose recordkeeping obligations on *everyone* involved in a blockchain transaction, such as mere software providers.

Responses to Specific RFC Questions

II. Greatest Risks and Key Trends in the Digital Asset Ecosystem

In your experience, what illicit finance risks and vulnerabilities pose the greatest risk in the digital asset ecosystem? What key trends in illicit finance risks have financial institutions observed in the digital asset ecosystem?

Introduction

While the vast majority of illicit finance occurs in the traditional financial sector, illicit cryptocurrency (or "**crypto**") transactions remain a concern for both industry and regulators alike. However, the greatest illicit finance risk in the crypto ecosystem is not the technology itself but the weak links that allow criminals to turn crypto back into cash: non-compliant offshore entities engaging in jurisdictional arbitrage, exploiting weak global regulations to help bad actors launder funds. At the same time, decades-old regulations like the BSA create an entirely different problem, by forcing financial institutions to over-collect and store vast amounts of sensitive personal information, which creates security vulnerabilities and places a burden on consumers.

We urge Treasury and Congress to prioritize enforcement efforts against non-compliant offshore entities and to modernize outdated regulatory frameworks, leveraging blockchain's inherent transparency and emerging privacy-preserving technologies. By fostering collaboration between industry and regulators, we can enhance the effectiveness of AML efforts, protect consumer privacy, and ensure the United States remains a leader in responsible digital asset innovation.

Non-compliant digital asset service providers and jurisdictional arbitrage

As Treasury acknowledged in 2024, the use of crypto for money laundering "continues to remain far below that of fiat currency and more conventional methods."[4] That said, much like traditional financial institutions, digital asset service providers ("**DASPs**")[5] face threats from a variety of bad actors seeking to exploit the financial system. So while illicit activity makes up a tiny fraction of overall crypto transactions,[6] ensuring that it remains low means DASPs must implement effective compliance programs. This requires adapting traditional controls - such as collecting "Know-Your-Customer" ("**KYC**") information and filing Suspicious Activity Reports ("**SARs**,") - to blockchain and other innovative technologies.

Bad actors prefer DASPs that require minimal (if any) KYC information, won't prevent their customers from exchanging funds with illicit counterparties, and won't respond to a government authority's request to freeze stolen funds. And the evidence demonstrates that these actors - ransomware groups, sanctioned entities, darknet markets, scammers, and other cybercriminals - have sought out non-compliant DASPs to monetize their crimes.[7] For this reason, the Financial Action Task Force ("**FATF**") and government authorities have repeatedly highlighted the threat that non-compliant DASPs pose.[8]

---

[4] U.S. Dep't of the Treasury, 2024 National Money Laundering Risk Assessment (Feb. 2024) https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf.

[5] While definitions of "digital asset service provider" or "virtual asset service provider" ("VASP") and similar terms vary, for present purposes this paper, we are using the definition of Digital Asset Service Provider as set forth in the GENIUS Act: "The term ''digital asset service provider''— (A) means a person that, for compensation or profit, engages in the business in the United States (including on behalf of customers or users in the United States) of— (i) exchanging digital assets for monetary value; (ii) exchanging digital assets for other digital Assets; (iii) transferring digital assets to a third party; (iv) acting as a digital asset custodian; or (v) participating in financial services relating to digital asset issuance; and (B) does not include— (i) a distributed ledger protocol; (ii) developing, operating, or engaging in the business of developing distributed ledger protocols or self-custodial software interfaces; (iii) an immutable and self-custodial software interface; (iv) developing, operating, or engaging in the business of validating transactions or operating a distributed ledger; or (v) participating in a liquidity pool or other similar mechanism for the provisioning of liquidity for peer-to-peer transactions." GENIUS Act, Pub. L. No. 119-27, S. 1582, 119th Cong. (2025).

[6] Chainalysis, *2025 Crypto Crime Trends* (Jan. 15, 2025), https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/ (estimating that the share of all attributed crypto transaction volume associated with illicit activity was 0.14% in 2024).

[7] Chainalysis, *Money Laundering Activity Spread Across More Service Deposit Addresses in 2023, Plus New Tactics from Lazarus Group* (Feb. 15, 2024), https://www.chainalysis.com/blog/2024-crypto-money-laundering/ ("While there are thousands of off-ramping services in operation, most money laundering activity is concentrated to a select few services. Of all illicit funds sent to off-ramping services in 2023, 71.7% went to just five services, up slightly from 68.7% in 2022.").

[8] *See, e.g.*, FATF, *Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs* (July 2024),

While a growing number of countries impose AML compliance obligations on DASPs, there are still large gaps in global enforcement efforts.[9] Some DASPs take advantage of these gaps by engaging in jurisdictional arbitrage - providing crypto services to global customers while having weak (or non-existent) AML controls, with the expectation that regulators will not hold them accountable.[10] A select few platforms are the preferred venues for sanctions evasion, terrorist financing, and large-scale money laundering.[11] A recent FATF implementation guide on digital assets called out the inconsistent global AML standards and requirements that allow for regulatory arbitrage and exploitation by large criminal networks.[12] In fact, Treasury recognized this tactic in its recent report on illicit finance, identifying the use of noncompliant DASPs as a "primary concern."[13] Treasury has also used its authority under Section 311 of the PATRIOT Act and Section 9714 of the Combating Russian Money Laundering Act to designate Cambodia-based Huione Group as a money laundering concern, and crypto exchange Bitzlato, alleging its ties to Russian illicit finance, respectively.[14] And the U.S. Department of Justice ("**DOJ**") has cautioned that "criminals continue to take advantage of noncompliant actors ... including noncompliant cryptocurrency exchanges ... to exchange their cryptocurrency for cash or other digital assets without facing rigorous [regulatory] scrutiny."[15]

Further, in failing to implement AML controls, non-compliant DASPs not only attract criminals; they also attract some customers who may simply choose the DASP with an onboarding process that is simpler and does not demand the collection of additional information. This, at least in the short term, gives non-compliant DASPs a competitive edge. Regulators are uniquely positioned to use their authority to ensure that DASPs

---

https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html; U.S. Dep't of the Treasury, *Action Plan to Address Illicit Financing Risks of Digital Assets* 13–14 (Sep. 20, 2022), https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf.

[9] *See* FATF, *Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* ¶¶ 26, 45 (July 2021).

[10] *See id.* 73.

[11] Chainalysis, *supra* note 7.

[12] FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* (June 2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf.

[13] U.S. Dep't of the Treasury, *supra* note 8.

[14] FinCEN, *Special Measure Regarding Huione Group, as a Foreign Financial Institution of Primary Money Laundering Concern*, 90 FR 18934 (proposed May 5, 2025), https://www.federalregister.gov/documents/2025/05/05/2025-07837/special-measure-regarding-huione-group-as-a-foreign-financial-institution-of-primary-money; FinCEN, *Imposition of Special Measure Prohibiting the Transmittal of Funds Involving Bitzlato*, 88 FR 3919 (Jan. 23, 2023).

[15] U.S. Dep't of Justice, *The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14607: The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related Digital Assets 7* (Sept. 6, 2022), https://www.justice.gov/ag/page/file/1535236/download.

throughout the world are held to the same standards and to root out illicit finance risks posed by this arbitrage. This approach can reap multiple benefits: regulators can ensure compliance with AML regulations; law enforcement can directly obtain records from DASPs in their jurisdictions (as opposed to having to use cumbersome methods to get records from overseas); and consumers gain by being able to use DASPs subject to the broad array of domestic regulatory protections.

One of the most effective ways to combat illicit finance, therefore, is to disrupt the ability of bad actors to cash out through the weak links in the system – the non-compliant banks, OTC desks, and crypto exchanges located in jurisdictions without robust AML requirements or enforcement efforts – making criminal behavior less profitable. We strongly support law enforcement receiving additional resources directed at prioritizing enforcement of AML and sanctions rules on non-compliant exchanges. For banks that are aiding in sanctions evasion as an on- or off-ramp, traditional sanctions authorities could also be applied.

Privacy risks posed by current regulations

While the greatest threat in the crypto ecosystems stems from non-compliant offshore DASPs, another critical risk stems from an unlikely source: outdated regulatory requirements that the BSA imposes on financial institutions, resulting in a system that unnecessarily jeopardizes the privacy of millions of Americans.

The BSA is a critical tool for finding bad actors and combatting illicit finance. The law is rooted in good intentions, but good intentions only go so far when technological advances outpace a former reality. This results in two critical vulnerabilities: (1) the risks posed when Americans share their sensitive personal information with numerous financial institutions, which are further compounded by (2) the risk of then sharing that information with regulators.

As to the former, for decades the BSA has required Americans to undergo mandatory KYC checks every time they sign up for a new account with a financial institution. That means their sensitive personal data has been shared with dozens of companies (and their partners). Thankfully, these financial institutions have mandatory safeguards, but safeguarding is imperfect and personal data is valuable. Beyond the annoyance customers feel every time they repeat the KYC process, these personal files – which companies are required by law to hold for years – are honeypots for criminals.

In addition to the risks posed by requiring private companies to hold vast troves of personal data, companies are also often required to share that data with regulators. The current system hinges on the Financial Crimes Enforcement Network's ("**FinCEN**") massive repository of people's financial records due to rules imposed in the 1970s. Each

year, the FinCEN database receives more than 25 million reports from financial institutions mostly on activity that carries no suspicion of illegality, such as withdrawing more than $10,000 in cash from a bank account.[16]

Although the FinCEN database was originally designed for the limited purpose of preventing Americans from using foreign banks to hide and launder money, today it puts ordinary Americans at risk by bulk-collecting their sensitive financial information and storing it in perpetuity. And Americans may be justifiably concerned about whether FinCEN can appropriately safeguard this data - particularly in light of reports that China was able to hack Treasury and gain access to the accounts of the former Treasury Secretary and her staff.[17] Further, in the past few years, several government employees have been prosecuted for leaking reports from the FinCEN database – a serious concern, particularly given that much of this information is rarely or never even used by law enforcement.[18]

Inefficiencies in Transaction Monitoring

Then there's the problem of transaction monitoring. Financial institutions are required to surveil every single transaction passing through their systems, in order to detect suspicious activity and then report it to the government. This sweeps in trillions of transactions, which must be reviewed by tens of thousands of people working for the financial institutions, who then decide whether to file a government report. The costs of these programs are passed on to customers in the form of higher banking fees, overly burdensome account opening requirements, and even denial of financial services. This is especially true for low-income customers, who are more likely to transact in cash and have more difficulty proving their sources of income. These high compliance costs also pose formidable barriers to entry for smaller financial service providers, including fintech startups, who need to build a business before establishing million-dollar compliance programs.

And to what end? In the U.S. alone, millions of reports flood Treasury and law enforcement agencies annually, yet the vast majority of them never result in a follow-up

---

[16] Cato Institute, *Reporting FinCEN's Suspicious Activity, Again* (July 9, 2025), https://www.cato.org/blog/reporting-fincens-suspicious-activity-again.
[17] Satter, R., *US Treasury says Chinese hackers stole documents in 'major incident'* (Dec. 30 2024), Reuters, https://www.reuters.com/technology/cybersecurity/us-treasurys-workstations-hacked-cyberattack-by-china-afp-reports-2024-12-30/.
[18] *See, e.g.,* Bank Policy Institute, *The Truth About Suspicious Activity Reports*, Sept. 2020, https://bpi.com/the-truth-about-suspicious-activity-reports/; Nicholas Kato, *GAO Report: DOJ Cannot Provide Meaningful Feedback on SAR Use*, Ballard Spahr (Sept. 2022), https://www.moneylaunderingnews.com/2022/09/gao-report-doj-cannot-provide-meaningful-feedback-on-sar-use/.

from law enforcement.[19] The inefficiency of this system is so well known that in 2020 Congress passed a law[20] requiring the Treasury Secretary to modernize this report-filing regime, yet little, if any, progress has been made.

The BSA is still rooted in decades-old requirements that reflect paper-based compliance protocols and a financial system in which funds moved over days, not seconds. But today funds can move instantly, and compliance teams are developing new ways to find bad actors. It would be a mistake to conclude, as some policymakers might, that the problem is the speed at which money can move – that's a feature, not a bug. Rather than blaming technology for an increase in problems, Treasury should be looking to technology for solutions.

Thankfully, there are better and safer options that already exist to update some of the key issues of the BSA - specifically, blockchain technology and ZK Proofs. Each of these technologies are discussed in greater detail below. But what bears emphasis here is that these technologies can arm the financial industry and regulators alike with more effective tools for combatting illicit finance while minimizing the risks posed by outdated elements of the BSA.

III. APIs

What innovative or novel methods, techniques, or strategies related to APIs are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to APIs?

a) **What factors do financial institutions consider when deciding whether to employ APIs for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use APIs for these purposes, what specific compliance functions do/will APIs support? For financial institutions that decided not to use APIs, please provide additional details on the rationale for that decision.**
b) **How are financial institutions using API tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of API tools with other existing or previous tools used for similar purposes.**
c) **Are there regulatory, legislative, supervisory, or operational obstacles to using APIs to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.**

[19] *See* Bank Policy Institute, *supra* note 18.
[20] AMLA, Div. F of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, Div. F, 134 Stat. 3388, 4547 (2021).

d) **What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of APIs for detecting illicit finance involving digital assets?**
e) **Treasury will evaluate APIs and consider their impact based on the research factors identified in the GENIUS Act. Provide any information pertinent to those factors.**

Introduction

Given the ubiquitous use of APIs across the financial services industry for AML/CFT and sanctions compliance, we encourage the U.S. government to foster public-private collaboration, support digital asset industry-led initiatives, and issue clear, technology-neutral guidance that promotes smart adoption of APIs for compliance purposes. Such efforts must be careful to avoid both imposition of overly-prescriptive requirements that stifle innovation around best use cases for APIs as well as creation of new obligations on top of existing ones.

The majority of software solutions in this field are API-based because APIs enable real-time data exchange, seamless integration with third-party tools, and the ability to scale compliance systems as transaction volumes grow. APIs allow financial institutions to connect to blockchain analytics platforms, sanctions screening databases, and transaction monitoring systems, creating a unified compliance ecosystem. This interoperability is critical in an increasingly complex regulatory environment, where institutions must process vast amounts of data quickly and accurately to detect illicit activity. The flexibility and efficiency of APIs make them the backbone of modern compliance programs, enabling institutions to adapt to evolving risks and regulatory requirements.

APIs play a critical role in Coinbase's efforts to detect and mitigate illicit finance risks in the digital asset ecosystem. By enabling seamless integration across systems and platforms, APIs enhance the effectiveness of Coinbase's AML and sanctions compliance programs. These tools are leveraged for real-time transaction monitoring, dynamic risk scoring, secure data sharing, and integration with advanced analytics solutions, ensuring Coinbase remains at the forefront of compliance innovation.

Transaction Monitoring and Blockchain Integration

Coinbase uses APIs to power its KYT controls, which uses blockchain analytics to dynamically assess transaction patterns and customer risk profiles. These APIs enable real-time transaction monitoring by integrating on-chain and off-chain data to identify red flags such as transactions involving high-risk jurisdictions, sanctioned addresses, or suspicious patterns. For example, APIs support Coinbase's real-time interdiction solution,

which can block transactions before they are completed, ensuring immediate action against sanctioned activity. Additionally, APIs are integral to Coinbase's blockchain analytics controls that leverage insight from multiple specialized vendors, providing visibility into the flow of funds and identifying links to illicit activities such as darknet markets or mixing services. These integrations allow Coinbase to trace transactions and investigate as needed. Further, APIs are used to deploy machine learning models that analyze transaction data for anomalies, enabling sophisticated risk detection.

TRUST APIs for Travel Rule Compliance

As another example, to comply with the "Travel Rule,"[21] Coinbase uses TRUST (Travel Rule Universal Solution Technology), which leverages APIs to securely share data with other DASPs. TRUST is the product of Coinbase's significant efforts (alongside other DASPs) to pioneer the development of a Travel Rule solution that allows DASPs to accurately identify their counterparties and securely share data. TRUST helps ensure that sensitive customer information is encrypted and transmitted safely, mitigating data privacy risks while maintaining compliance with regulatory requirements. This API-driven solution allows Coinbase to exchange Travel Rule data seamlessly across jurisdictions, reducing friction in cross-border transactions and enhancing the overall security of the digital asset ecosystem.

Importantly, Coinbase engaged closely and repeatedly with FinCEN and other regulators while designing and expanding TRUST. Treasury should prioritize this collaborative approach, specifically to further facilitate effective, risk-based adoption of APIs for compliance purposes. Collaboration with DASPs will allow both parties to more efficiently integrate new solutions – such as use of APIs by TRUST for Travel Rule compliance – into compliance and regulatory work.

Benefits and Safeguards of APIs

The use of APIs provides Coinbase with enhanced detection capabilities, scalability, and interoperability, while also reducing manual intervention and operational costs. However, Coinbase recognizes the risks associated with APIs, such as data privacy concerns, regulatory compliance challenges, and reliance on third-party providers. To mitigate these risks, Coinbase employs robust safeguards, including encryption, role-based access controls, regular audits, and vendor due diligence. For example, TRUST APIs use encryption to ensure that sensitive data remains secure during transmission.

[21] 31 C.F.R. § 1010.410(f).

Recommendations

To promote the effective and risk-based adoption of APIs in the detection of illicit finance within the digital asset ecosystem, the U.S. government should consider the following comprehensive steps:

- **Foster Ongoing Public-Private Collaboration** - Establish structured, recurring forums and working groups that bring together regulators, DASPs, technology vendors, and other stakeholders. These forums should focus on sharing intelligence about emerging threats, discussing technical and operational challenges, and developing best practices for API implementation. One critical example could be developing an API feed of known illicit crypto addresses fed by Internet Crime Complaint Center ("**IC3**") and FinCEN data that could be integrated into financial institutions' compliance regimes to help them stop new transfers to scammers and fraudsters. Open lines of communication will help ensure that regulatory approaches remain informed by real-world developments.

- **Provide Clear, Technology-Neutral Regulatory Guidance** - Issue guidance that articulates regulatory objectives and compliance outcomes without mandating specific technical solutions or architectures. This approach allows exchanges and other market participants to innovate and adopt the most effective API-driven tools for their unique business models and risk profiles. Clear guidance should also address data privacy, cross-border data sharing, and the use of third-party vendors, reducing uncertainty and enabling more confident investment in compliance technology.

- **Support and Endorse Industry-Led Standardization Initiatives** - Encourage and, where appropriate, participate in the development of industry-wide standards for API protocols, data formats, security measures, and interoperability. Standardization reduces fragmentation, lowers integration costs, and enhances the effectiveness of information sharing across the ecosystem. The U.S. government can play a constructive role by endorsing widely adopted standards, which will incentivize broader adoption and facilitate cross-institutional collaboration.

- **Expand Regulatory Sandboxes and Pilot Programs** - Create or broaden regulatory sandboxes and pilot initiatives that allow exchanges and technology providers to test innovative API-based compliance solutions in a controlled environment that would replace outdated, manual reviews and other labor-intensive processes. These programs should offer regulatory flexibility, constructive feedback, and a safe space to experiment with new approaches to transaction monitoring, sanctions screening, and data sharing. Insights gained from these pilots can inform future rulemaking and help identify best practices before broader implementation.

- **Ensure Proportionality and Minimize Unnecessary Burdens** - When developing new requirements or evaluating the effectiveness of API-driven compliance tools, regulators should carefully assess the actual risks posed by specific activities and technologies. Requirements should be tailored to address those risks without imposing excessive operational or technical burdens that could stifle innovation or limit access to digital asset services. Ongoing cost-benefit analysis and stakeholder consultation will help ensure that compliance measures remain both effective and efficient.

- **Promote International Coordination and Harmonization** - Given the global nature of digital assets, the U.S. government should work with international counterparts to harmonize regulatory expectations and technical standards for API use in AML/CFT compliance. This will facilitate cross-border data sharing, reduce regulatory arbitrage, and support a level playing field for U.S.-based firms operating internationally

By taking these steps, the U.S. government can help ensure that API adoption in the digital asset sector is both effective in combating illicit finance and supportive of continued innovation and growth.

IV. Artificial Intelligence

What innovative or novel methods, techniques, or strategies related to AI are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to AI? Please describe the use of AI to conduct analysis of transactional data, including transactions that occur on blockchains, and to identify complex illicit financial networks, as well as key lessons learned from use of AI in this context.

a) **What factors do financial institutions consider when deciding whether to employ AI for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use AI for these purposes, what specific compliance functions does/will AI support? For financial institutions that decided not to use AI, please provide additional details on the rationale for that decision.**
b) **How are financial institutions using AI tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of AI tools with other previous or existing tools used for similar purposes.**
c) **Are there regulatory, legislative, supervisory, or operational obstacles to using AI to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.**

d) **What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of AI for detecting illicit finance involving digital assets?**
e) **Treasury will evaluate AI and consider its impact based on the research factors identified in the GENIUS Act. Provide any information pertinent to those factors.**

Introduction

The on-chain ecosystem of digital assets offers unprecedented opportunity for compliance programs to leverage advancements in AI to combat illicit finance. But realizing this potential requires updating the BSA, which remains rooted in decades-old requirements that reflect paper-based compliance protocols and a financial system that takes days to settle fund transfers through clearing houses and correspondent banking rails, instead of atomistically on a blockchain.[22]

Coinbase is one of many DASPs that has moved beyond traditional, static rule-based systems to address the complexities of modern financial crime. This shift, if embraced by regulators through issuing updated rules and guidance, is poised to enhance the effectiveness of AML/CFT efforts and redefine the compliance landscape. The key enabler is the blockchain's transparent and immutable ledger, which allows the full lifecycle of an asset's movement and activity to be continuously processed by blockchain analytics platforms, including through the use of machine learning ("**ML**") algorithms. This offers far greater risk assessment opportunities than traditional AML methods, allowing firms to better meet their regulatory obligations while also helping regulators fulfill their missions.

To reach the full promise of AI, however, regulated entities need clear guidelines on how to manage new risks related to data privacy, bias, and explainability, all of which necessitate a careful and coordinated response from both industry and the government. Treasury and other regulators must consider both issuing guidance that promotes

[22] Paul Grewal, *The Bank Secrecy Act Is Broken. Technology Can Fix It*, Coinbase Blog (Aug. 4, 2025), https://www.coinbase.com/en-de/blog/the-bank-secrecy-act-is-broken-technology-can-fix-it.

responsible use of AI - a move already being taken by other global regulators[23] - and also look for ways to collaborate with and learn from the digital asset industry as new uses for AI emerge.

This response describes the innovative applications of AI in detecting illicit finance, examines the multifaceted risks and benefits of its adoption, and explores the regulatory and operational considerations that will shape its trajectory.

Innovative AI Applications for Illicit Finance Detection and Network Analysis

Financial institutions are increasingly employing novel, AI-powered techniques to enhance their defenses against illicit finance, especially within the digital asset ecosystem. These approaches allow for the analysis of vast datasets to identify intricate financial networks and detect criminal activity that would be impossible to uncover using conventional tools alone.

Effectiveness of Blockchain Analytics for KYT

A key compliance program innovation is the shift from reliance on static, simple rules-based controls toward dynamic, ongoing monitoring of on-chain activity. Unlike traditional AML methods that rely solely on information from a closed-ledger environment, KYT programs use advanced heuristics (and in some cases ML methods) to process the data from public blockchains, allowing for a robust and repeatable basis for sanctions and AML analytics. With their ability to analyze vast amounts of data, these platforms digest blockchain data for prevention of illicit activity and use emerging technology to continuously improve upon established methods of using data analytics to check on-chain payments and transactions for suspicious patterns and potential financial crime.

A cornerstone of this innovative toolkit is graph analytics, a method that maps out the relationships between entities such as individuals, companies, wallet addresses, and transactions. By visualizing these connections, tied together by immutable blockchain records, DASPs can uncover multi-layered illicit networks that are not readily observable

[23] For example, the UK's ongoing efforts to keep pace with AI developments through its consultations, white-papers, and guidance documents. *See* UK Gov't, *A Pro-Innovation Approach to AI Regulation* (2023), https://www.fca.org.uk/publication/corporate/ai-update.pdf *; EU AI Act overview, European Parliament* (2023), https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response ("Harnessing AI for the benefit of humans and businesses alike has rightly become a priority of Governments, policy makers and regulators everywhere. The UK has a head start provided by world-class universities, brilliant cities and businesses attracting global talent, with internationally respected institutions.").*See also* EU AI Act overview, European Parliament (2023), https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence#encouraging-ai-innovation-and-startups-in-europe-4 (providing a comprehensive framework for AI use).

in traditional financial system records, thus revealing otherwise hidden relationships.[24] ML models can continuously process this richer dataset and surface real-time signals, allowing the DASP to intervene earlier, as opposed to traditional tools that lack these capabilities.[25] This analysis would be particularly powerful when enriched with other government datasets of illicit activity such as reports sent to IC3 of victims of fraud or SAR filings with FINCEN.

For example, most blockchain analytics and forensic companies deploy ML and AI to differing extents, including Blocktrace, Arkham, Elliptic, TRM Labs, Nansen, and Chainalysis. Blocktrace has developed AI to interact with the Bitcoin blockchain, so that users can quickly access specific data points including Bitcoin addresses, transaction dates and values. Instead of having to program using advanced, technical language to search the blockchain, users can use a chatbot that's already trained on the data to find the results they need.[26]

Customer Onboarding and Fraud Prevention

Like many other financial institutions, Coinbase is also exploring the use of AI systems to improve the overall customer experience, particularly in the areas of customer onboarding and fraud prevention. This is where ML models can automate the identity-verification process and mitigate fraud risk that may be more likely caused by human error.

For instance, an ML model can ingest a customer's photo and other documents, comparing them to a real-time photo and other public domain images to create a safer experience. Once a customer is onboarded, ML models continue to analyze data inputs like name changes, linked accounts, unusual transactional activity, and immediate asset transfers to identify second- and third-party fraud. ML also can be used to automate protective actions (e.g., account or transaction holds/freezes), significantly enhancing the efficiency and effectiveness of our AML program.

Additionally, large language models in AI systems are exceptionally valuable for fraud detection due to their ability to establish connections between user patterns and profiles, enabling them to efficiently identify patterns that might be out of character. Those

---

[24] *See, e.g.*, New Lines Institute, *Chinese Shadow Liquidity and the Scam Economy* (Sept. 2025), https://newlinesinstitute.org/state-resilience-fragility/chinese-shadow-liquidity-and-the-scam-economy/ (explaining how Chinese Triads, with deep roots in gambling, now use both physical and online casinos to launder cartel funds. Crypto is accepted for gambling credits, which are then cashed out as "winnings" or business revenue, further muddying the money trail. This casino-based laundering is a growing vector for both drug and human trafficking proceeds.)
[25] *See, e.g.*, Coinbase, *Response to U.S. Treasury RFI on AI in Financial Services* (Aug. 12, 2024), https://assets.ctfassets.net/o10es7wu5gm1/6uO6LHCnY5Rm7fYeiM3R6P/f99c7948d2445605917348e10e9b7422/2024-08-12-UST_RFI_on_Artificial_Intelligence.pdf.
[26] *Id.*

algorithms can then be deployed in real-time and become more predictive as they spot patterns and make decisions that separate signal from noise.[27]

Market Surveillance and Integrity

Similarly, in market surveillance, AI models are trained on large quantities of data to recognize patterns and deviations, helping to detect manipulative trading activities such as "spoofing" or "layering." Coinbase's spot crypto and derivatives exchanges have observed substantial efficiency gains in running their respective trade surveillance programs with these tools. The techniques enable 24/7/365 monitoring across all of Coinbase's trading platforms in a way that manual tracking alone cannot match. Unlike traditional market surveillance, which is often done forensically after the fact, ML provides Coinbase's trade surveillance teams with real-time insights that can be actioned and quickly mitigated, offering a substantial efficiency gain over manual, forensic-only surveillance methods.

Risks and Regulatory Obstacles

Other countries and regions have been issuing principles-based, AI-related guidance that, while not necessarily frameworks aligned with what would be most appropriate for the U.S., has at least provided some clarity around regulatory expectations. The UK government, for example, adopted a cross-sector and outcome-based framework for regulating AI[28] and the Artificial Intelligence Act of the EU governs the development and use of AI in the EU that takes a risk-based approach to regulation, applying different rules to AI according to the risk they pose.[29]

The accelerating adoption of AI in financial services, while offering significant benefits, also introduces a complex set of risks that must be carefully navigated. The biggest frictions are not technical but governance-related: (i) overly prescriptive AI rules risk stifling innovative applications of AI; (ii) third-party opacity makes it hard to verify data handling and model behavior without access controls and audit rights; and (iii) production AI still demands human-in-the-loop review, quality assurance, and continuous monitoring for drift and bias. While the benefits of AI are undeniable, it is important for financial institutions to incorporate AI models responsibly, for example, by adopting risk-management programs and controls to protect customer privacy.

---

[27] Coinbase Institute, *Blockchain and Artificial Intelligence (AI): Complementary Technologies That Can Make Each Other Better*, https://www.coinbase.com/en-de/public-policy/advocacy/documents/blockchain-and-ai.
[28] *See* UK Gov't, *A Pro-Innovation Approach to AI Regulation* (Aug. 3, 2023), *supra* note 23.
[29] *See* European Parliament, *EU AI Act: First Regulation on Artificial Intelligence* (2023), https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

Finally, laws or guidance that create complex or potentially unclear expectations for the use of AI may favor a small set of large firms with the resources necessary to successfully navigate them. This would serve to entrench incumbent entities while limiting contributions from more innovative newcomers.

Recommendations

A pragmatic path forward is a principles-based supervision regime that focuses on outcomes – such as alert precision and interdiction speed – and good governance, including human oversight, testing, and vendor transparency, rather than mandating specific models or pipelines. Treasury can accelerate safe adoption by:

- Issuing regulations and guidance that provide the industry with clear parameters to follow when seeking to adopt this technology – specifically, in the form of regulatory safe-harbor within the BSA – that will encourage exploration and use of AI.

- Acknowledging that the use of ML models is a compliance enabler and encouraging responsible integration of on-chain with off-chain data, including guidance on handling obfuscation tools and confidence scores.

- Supporting public-private information sharing and, where feasible, labeled datasets for model validation, potentially by leveraging the existing FinCEN 314(a) and 314(b) information-sharing mechanisms.

- Acknowledging that where implemented adequately, supervising regulators can expect that such models could result in a decrease in alerts but an increase in actionable SAR filings.

- Having FinCEN implement its own AI model for reviewing/scoring incoming SAR filings and then provide that feedback directly to the filing institution through the use of APIs so that the FI can calibrate and improve its own AI-based transaction monitoring systems and SAR filing processes. This FinCEN AI model could be further enhanced with a feature to capture feedback from any law enforcement or regulatory agencies who subsequently review and score the filing. Such direct feedback would help improve the FIs controls and reduce the incidence of law enforcement/regulators receiving less useful SAR filings.

- Publishing a consultation or white paper promoting underlying principles and taking a pro-innovation approach, as has been done in the UK.[30]

[30] *See* UK Gov't, *A Pro-Innovation Approach to AI Regulation* (2023), *supra* note 23.

Crypto markets, more so than other financial markets, are truly global. As a consequence, crypto markets require a significant degree of cross-border regulatory cooperation and harmonization. This applies to rules surrounding the use of AI-based systems as well. For example, to the extent we use ML models to monitor trading or fund flows, it is not clear how more restrictive rules on the use of AI in one jurisdiction would impact our global monitoring program. Further, by incentivizing AI-based compliance solutions, Congress can help make regulatory compliance more effective, less costly, and more protective of user data across the entire financial system.

GENIUS Act Research Factors

We set forth below ways that the use of AI relates to and impacts certain research factors Congress identified in the GENIUS Act.

- **Improving Detection of Illicit Activity** - As discussed above, AI combined with blockchain analytics has improved precision and speed in identifying and addressing illicit financial activity, as well as in attribution of addresses controlled by sanctioned actors. AI is also helping improve other customer touchpoints such as onboarding, as well as playing a role in preventing fraud.
- **Costs to Financial Institutions** - Many financial institutions have already incorporated ML processes into their compliance programs. Up-front integration and expertise-building costs are significant but eventually offset by reduced manual review and better alert quality over time.
- **Data and Privacy Risks / Cybersecurity** - Financial institutions can limit data exposure and privacy risks via minimization of unnecessary data exposed to AI models, segmentation of models to further reduce data leakage concerns, and strict third-party vendor terms (e.g., zero-retention, scrubbed logs, plus audit rights to verify compliance).
- **Overall Effectiveness and Efficiency** - ML models have already significantly improved the effectiveness of mitigating illicit finance. Combining ML with on-chain “ground truth” data yields a more robust, repeatable basis for sanctions and AML analytics than closed-ledger environments utilizing traditional review tools alone, while providing better alert quality and helping reallocate human review to higher-risk compliance activities.

V. Digital Identity

What innovative or novel methods, techniques, or strategies related to digital identity verification are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to digital identity verification? Please describe the portable digital identity credentialing tools in use and how such tools are being used.

a) **What factors do financial institutions consider when deciding whether to employ digital identity verification for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use digital identity verification for these purposes, what specific compliance functions does it/will it support? For financial institutions that decided not to use digital identity verification, please provide additional details on the rationale for that decision.**
b) **How are financial institutions using digital identity verification tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of digital identity tools with other existing or previous tools used for similar purposes.**
c) **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.**
d) **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?**
e) **Treasury will evaluate digital identity verification and consider its impact based on the research factors identified in the GENIUS Act. Provide any information pertinent to those factors.**

Introduction

Digital identity verification is a critical tool for advancing both financial compliance and innovation in the digital asset ecosystem. We urge policymakers to modernize existing regulations to explicitly recognize advanced digital identity solutions, such as decentralized identity and zero-knowledge proofs, as valid methods for AML/CFT compliance. By providing regulatory clarity and expanding reliance frameworks, the U.S. can enhance the effectiveness of illicit finance detection while reducing unnecessary burdens on industry, fostering a secure, inclusive, and globally competitive digital economy.

History of Identification and the Rise of Digital ID

Forms of identification have evolved over time, from official papers verified by watermarks to personal ID numbers and photo identification. With the advent of the internet in the 1990s came the rise of "digital IDs." These IDs are often in the form of a username and password that provide entry to a particular website, thus granting access to critical information like your bank account or healthcare information. Digital IDs can also be used offline, such as in the form of a digital driver's license.

Digital IDs are convenient because they can be authenticated online and therefore make it possible to access services remotely. But simply digitizing a business process or physical ID doesn't necessarily improve user privacy or security, and in many instances introduces additional risks from hacking and cybercrime. This is true whether digital IDs are stored and managed in discrete "silos" by different organizations, or stored and managed by a "federated" cloud service:

- **Siloed**: Under the initial "siloed" digital ID approach, each website or organization issues its own ID to users in the form of username/password combinations. This approach requires users to remember or manage many unique usernames and passwords. It also leads to extensive data duplication across multiple websites and databases, all of which are prime targets for hacking and identity theft.
- **Federated**: In response to shortcomings from the siloed model, organizations developed a "federated" approach, where companies like Google issue digital ID credentials that work across a variety of websites and services. This model makes online identity verification more convenient. But it concentrates personal data in the hands of a few central authorities that operate the federated entry point, raising additional concerns about privacy and security.

Services that issue a federated digital ID compromise privacy through their practices of collecting, storing, and sharing large amounts of user data. The process starts by collecting data directly from the user, like name, birthdate, address, and sensitive answers to security questions. This is then combined with other information about the user, like geolocation data and browsing history, which is tracked and collected by the service provider, often without the user's knowledge. The combined data is ultimately stored and replicated hundreds of times in different databases, one for each website or service where a user has registered. This data can also be shared with other companies for profit, without the user's consent.

Both the siloed and federated approaches raise serious security concerns. Storing personal information in countless different silos inherently increases vulnerability to hacking and cybertheft. Different websites have varying password and authentication requirements, and as security and identity protocols change over time, it's nearly

impossible to consistently update disparate identity silos in unison, thereby increasing security risks.

Decentralized ID

Decentralized ID, or "**DiD**", offers a new form of identity management that relies on blockchain technology to solve the security, privacy, and consent issues presented by paper and digital IDs. It is a credential that a user holds in a digital wallet that proves certain characteristics about their identity, but without necessarily providing the underlying details of the proof – like age, address, or Social Security Number ("**SSN**"). This gives individuals control over who has access to their personally identifying information ("**PII**"), and offers an alternative to outsourcing identity management to a single centralized authority like the government or big tech.[31]

The enhanced privacy, control, and portability offered by DiDs help protect against myriad illicit finance risks. Customers are safer in a KYC environment that requires less re-collection of PII and sharing of specific documentation and details. It can replace traditional KYC practices developed in the context of opaque transactional ledgers and customer records, held by one firm and inaccessible to others. Notably, it removes both (1) the risk and redundancy from each firm relying on its own identity verification processes, often operationally executed through multiple third-party vendors; and (2) the need for customers to provide their personal information to every financial institution they wish to open an account with.

A key innovation to DiD solutions is the use of ZK Proofs.[32] ZK Proofs use cryptography to enable a trusted party, such as a regulated financial institution, to verify certain information about an individual (such as a birthdate, SSN, or the fact that they have undergone full KYC as of a certain date). The financial institution issuing the credential underlying the ZK Proof provides the customer with an attestation token confirming the facts at issue. The customer, Jane Smith, can then use it when interacting with other entities that need to confirm the same fact - for example, that she is a U.S. citizen - without necessarily having to disclose anything additional about herself.[33] And if law

---

[31] For more discussion of these legacy methods of digital identification, *see* Coinbase Institute, *Primer: Decentralized Identity*, https://www.coinbase.com/en-nl/public-policy/advocacy/documents/decentralized-identity.
[32] *See* Ethereum.org, *What are Zero-Knowledge Proofs?*, https://ethereum.org/en/zero-knowledge-proofs/ (describing how a "zero-knowledge proof allows you to prove the truth of a statement without sharing the statement's contents or revealing how you discovered the truth," utilizing "algorithms that take some data as input and return 'true' or 'false' as output.").
[33] *See also* FATF, *Guidance on Digital Identity* 107 (Mar. 2020), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf (describing how digital ID systems can also provide more efficient experience for customers).

enforcement wanted detailed information on the customer, they would be able to subpoena the company that issued the ZK Proof.[34]

Similarly, a new financial institution opening an account for Jane could use her attestation token from a DASP that has already conducted full KYC on her. This streamlines the KYC process and frees up compliance resources for other effective compliance activities – for example, monitoring and investigating suspicious transactions.[35] Further, if Jane engaged in activities that increase her risk profile, or if her previously confirmed identifiers change, the original financial institution could modify the attestation token to reflect those changes. DASPs can also incorporate all types of blockchain data into an attestation token, such as aggregate transactional information, to create a dynamic, evolving picture of the customer's risk profile. Additionally, DiD could be used by DeFi smart contracts to gate access: digital identity tools can allow smart contracts to automatically check for a credential before executing a user's transaction.

More broadly, DiD also has the potential to create a more inclusive and streamlined economy. More than one billion people worldwide lack formal identification,[36] which can limit access to essential needs like healthcare or financial services. DiD allows anyone with internet access to provide proof of their name, birthdate, work experience, and more, quickly providing a verified means of identification controlled by the user. And DiD also provides clearer audit trails for both firms and regulators alike.

Regulatory Obstacles and Other Challenges

Regulation needs to keep pace with DiD's potential. In the United States, for example, the BSA currently requires financial institutions to take certain steps to know who their customers are. For instance, banks are subject to what is known as the Customer Identification Program ("**CIP**") rule,[37] while money services businesses ("**MSBs**") must abide by general KYC requirements.[38] Under the CIP rule, a bank can verify a customer's identity using "non-documentary methods" - in other words, methods other than government-issued IDs or similar documents.[39] But neither the CIP rule nor regulators' guidance to date clarifies whether DiD would qualify as a suitable "non-documentary method."

---

[34] *See* Ethereum.org, *supra* note 32.
[35] *Id.* (recognizing that the use of digital ID systems could reduce customer onboarding costs up to 90%, enabling entities to "allocate compliance resources to other [AML] compliance functions, and also facilitate financial inclusion for otherwise excluded or under-served individuals by reducing on-boarding costs.").
[36] World Bank, *Principles on Identification for Sustainable Development*, at 3 (Feb. 2021), https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf.
[37] 31 C.F.R. § 1020.220.
[38] 31 C.F.R. § 1022.210(d)(1).
[39] 31 C.F.R. § 1020.220(a)(2)(ii)(B).

A similar ambiguity surrounds whether a DASP in the United States - which is often registered as an MSB - could rely upon DiD to help satisfy its obligations under the KYC rule. The result is that private industry has been hesitant to take the necessary steps to more fully embrace DiD. Further, while the CIP rule allows banks to rely on verifications provided by other financial institutions, the rule strictly limits which *kinds* of other financial institutions a bank could rely on - specifically, only a limited class of institutions subject to a "federal functional regulator," which excludes MSBs and other firms that could offer DiD services.[40]

Treasury's prior efforts to promote the development of novel identity tools are commendable.[41] And more work should be done on this front. But until the underlying regulations are modified, or regulators issue guidance clarifying how firms can meet CIP and KYC obligations using DiD, it is unlikely that industry will be able to fully integrate DiD into their compliance programs, which would enhance overall efforts to disrupt illicit activity.

This process must also be global. Governments around the world are already beginning to embrace DiD to develop faster, more secure, and more readily accessible services.[42] Many innovative projects are underway that will change how we hold and share information about our personal identity, providing tangible benefits for individuals and institutions. As exploration in this space continues, regulatory clarity is needed so that individuals and private industry are comfortable innovating, embracing, and adopting DiD for daily use. To avoid fragmentation, regulatory arbitrage, and duplicative compliance burdens, Treasury should also use the U.S. delegation to the FATF to champion the use of DiD and privacy-preserving tools such as ZK Proofs as a valid means of customer due diligence and ongoing monitoring.

Meanwhile, integration of DiD into compliance efforts presents several challenges. First, without expanded access and education, digitization of identity could further deepen the digital divide. DiDs must be usable by everyone, regardless of their economic status or

---

[40] *See* 31 C.F.R. § 1020.220(a)(6)(ii).
[41] *See* Press Release, FinCEN, 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 (describing Treasury's "Tech Sprint" and efforts to understand how to use digital identity proofing to reduce money laundering and terrorist financing).
[42] *See, e.g.*, European Self-Sovereign Identity Framework Lab, The EU Project eSSIF-Lab, https://essif-lab.github.io/framework/docs/essifLab-project (describing a European Union-funded project to advance new generations of digital identity solutions); California Blockchain Working Group, Blockchain in California: A Roadmap, 2 (July 1, 2020), https://www.govops.ca.gov/wp-content/uploads/sites/11/2020/07/BWG-Final-Report-2020-July1.pdf (outlining the government of California's potential use of blockchain and digital identification technology with respect to the Department of Motor Vehicles records).

technological know-how. DiDs offer more privacy and control, but in turn they place more responsibility on individual users to manage their credentials.

Second, DiD developers must ensure DiD systems can work together seamlessly. There are currently over 100 DiD systems in development, each with its own architecture and digital wallet.[43] It is crucial that systems develop a seamless protocol for exchanging credentials, so that people can interact freely with employers, financial institutions, healthcare providers, and others that both issue and verify credentials. To do this, DiD systems must agree on standards for foundational elements of DiD architecture.

The U.S. regulatory landscape has not kept pace with DiD, creating uncertainty that discourages adoption by financial institutions. Moreover, the existing AML framework under the BSA requires the collection of vast sums of sensitive customer data; use of DiD offers the opportunity to modernize these antiquated, burdensome obligations.[44] As discussed in more detail above, the two principal obstacles in the existing regulatory framework relate to: (1) ambiguity around whether DiDs would qualify as "non-documentary" verification under the CIP Rule, and (2) the CIP reliance framework,[45] which restricts the ability of many financial institutions to leverage identity verification work already completed by other institutions to narrow class of financial institutions that are regulated by federal functional regulators and meet other requirements.[46]

On the reliance issue, MSBs such as Coinbase are not regulated by federal functional regulators. Thus, while they are particularly well-positioned to develop DiD onboarding tools, they cannot participate in sharing it or relying on others' use of it. The ability to leverage this verification work is a key benefit (and in many ways, the core principle) of DiD – and under today's framework would not be available to many DASPs that are MSBs. As a result, a bank or DASP cannot efficiently accept a DiD credential previously issued by another DASP that has already conducted a full KYC check. This results in duplicative work, increased costs, and friction for consumers. This legal uncertainty makes financial institutions hesitant to fully invest in and integrate DiD into their compliance programs, even though it would enhance overall efforts to disrupt illicit activity.[47]

---

[43] Nextrade Group, *Supporting Digital Transformation and Economic Growth Through Interoperable Digital Identity* (June 2025), https://www.nextradegroupllc.com/interoperable-digital-ids.
[44] Grewal, *supra* note 22.
[45] 31 C.F.R. § 1020.220(a)(6) (reliance provision available to banks and certain other financial institutions but not MSBs).
[46] *See* FDIC, *Customer Identification Program*, 7-8, https://www.fdic.gov/news/financial-institution-letters/2021/fil21012b.pdf.
[47] Coinbase,, *Ensuring Responsible Development of Digital Assets; Request for Comment* (Nov. 2022), https://assets.ctfassets.net/c5bd0wqjc7v0/4QJpib4JJ4AYCpOiuYavSP/3670f91940053f7e16760d1d74f9051f/Coinbase_Comments_-_Treasury_RFC.pdf .

Recommendations

Under the BSA, the rules around onboarding and identity verification restrict the approaches financial institutions may take, particularly with respect to use of DiD. There is no guidance on the use of DiD to achieve identity verification, and the CIP Rule provision allowing for reliance on others' KYC results is extremely limited. Treasury and Congress should consider making updates to these BSA requirements to support the utilization of DiDs to improve AML/CFT and sanctions compliance efforts, increase efficiency, and reduce privacy and data breach risks for consumers.

- **Issue updated regulatory guidance**: Formal guidance should be issued, or the existing CIP Rule updated, to clarify that DiD and other cryptographically-secured digital identity credentials are a permissible "non-documentary method" for satisfying CIP and KYC requirements.[48] This could also happen through specific changes to the language in the verification section of the CIP Rule, thereby further removing ambiguity. Such a change would provide the legal certainty necessary for widespread industry adoption of DiD.
- **Modernize and expand the CIP and CIP reliance framework**: The reliance framework should be updated to allow all financial institutions to rely on the identity verifications conducted by a broader range of regulated entities, including MSBs. This would enable the creation of an interoperable identity ecosystem where a customer's verified identity can be securely and efficiently reused, streamlining onboarding and freeing up compliance resources to focus on higher-risk activities.
- **Prioritize decentralization and adaptation:** Any regulatory updates or guidance supportive of DiD also should not allow a single, issuing agency to control the issuance or verification of credentials.[49] It is equally important that identifiers be unique to each individual globally, and be updateable as technology continues to mature.[50]

By implementing these changes to existing AML laws and guidance, regulators can foster innovation and enable the financial industry to integrate advanced digital identity solutions into their AML/CFT programs.

---

[48] *See* Coinbase Institute, *supra* note 31.
[49] *Id.* (citing the Worldwide Web Consortium (https://www.w3.org/) and Decentralized Identity Foundation (https://identity.foundation/) as having identified this, among several other key principles essential to DiD).
[50] *Id.*

VI. Blockchain Technology

What innovative or novel methods, techniques, or strategies related to blockchain technology and monitoring are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to blockchain technology and monitoring? Please describe how financial institutions are integrating information from blockchain analytics with off-chain data and mention any key challenges associated with using blockchain analytics (e.g., obfuscation tools and methods that can complicate tracing and assessing confidence in attribution or complexities inherent in cluster analysis).

a) **What factors do financial institutions consider when deciding whether to employ blockchain technology and monitoring for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use blockchain technology and monitoring for these purposes, what specific compliance functions does it/will it support? For financial institutions that decided not to use blockchain technology and monitoring, please provide additional details on the rationale for that decision.**
b) **How are financial institutions using blockchain technology and monitoring tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of blockchain technology and monitoring tools with other existing or previous tools used for similar purposes.**
c) **Are there regulatory, legislative, supervisory, or operational obstacles to using blockchain technology and monitoring to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.**
d) **What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of blockchain technology and monitoring for detecting illicit finance involving digital assets?**
e) **Treasury will evaluate blockchain technology and monitoring and consider their impact based on the research factors identified in the GENIUS Act. Provide any information pertinent to those factors.**

Introduction

Blockchain technology is transforming AML and sanctions compliance by giving DASPs unprecedented transparency and analytical power. Unlike traditional financial institutions, DASPs can use public, immutable blockchain data to monitor transactions beyond their own platforms, enabling real-time, independent, and dynamic risk assessments. This enhances transaction monitoring, customer risk ratings, and sanctions screening, reducing false positives and improving suspicious activity reporting. To maximize these benefits, regulations should remain technology neutral and focused on custodial intermediaries. Further, policymakers should support law enforcement with additional resources and advanced tools, encourage information sharing, and recognize the blockchain's value in compliance. Integrating new innovations with traditional measures enables financial institutions to operate more efficiently, protect privacy, and better combat illicit finance.[51]

Unprecedented Compliance Benefits of Blockchain Technology

In many countries around the world, financial institutions are already required to implement effective AML programs. For example, in the United States the BSA requires financial institutions to collect KYC information, monitor incoming and outgoing transactions, and file SARs, among other responsibilities. These requirements apply equally to traditional financial institutions and DASPs.

But the emergence of crypto over the last decade has given DASPs a powerful new set of compliance tools to radically enhance their effectiveness at identifying and disrupting illicit finance. These new tools harness the public and transparent nature of the blockchain, allowing DASPs to track the flow of assets beyond what happens on their individual platforms, thus giving them a far deeper and richer understanding of the risks posed by specific transactions and customers. Blockchain data can then be combined with traditional compliance tools to enhance transaction monitoring and screening, customer risk ratings, SAR filings, and market integrity, all leading to a more effective level of compliance.

Blockchains collect all transactions and record them on a common, public ledger. While traditional financial institutions have limited ability to see off-platform transactions, with blockchains off-platform activity is available by default. This means that DASPs (along with regulators and law enforcement) can analyze transactions carried out on the

[51] This response draws from materials previously presented by current and former Coinbase staff, and which contain more information on the effective use of blockchain technology to combat illicit finance. *See* Christiansen, et al., *AML for a Blockchain Age*, Journal of Financial Compliance, 7 (2), 148-159 (2023).

blockchain - whether or not they took place on the DASP's own platform.[52] For example, if a bank's client wants to deposit funds into an account, the bank must rely on information provided by the customer about the source of those funds, instead of being able to independently and immediately review historical activity on the blockchain. In short, crypto fixes this problem for traditional finance by giving DASPs unprecedented access to a much fuller scope of transactional records.[53]

This additional data (not limited by private ledgers) lets DASPs conduct sophisticated analyses to determine the risk of a specific transaction or asset - using tools and methods broadly referred to across the crypto ecosystem as blockchain analytics. For example, such tools and methods include the use of machine-learning algorithms trained on massive sets of blockchain and other data. An entire industry of blockchain analytics firms have developed KYT and other blockchain analytics products in recent years to assist DASPs and law enforcement in utilizing the treasure-trove of data held in blockchains.[54] KYT is groundbreaking for compliance because it is *immediate* (the information is available on the blockchain), *independent* (it does not have to come from the customer and cannot be tampered with), and *dynamic* (the risk associated with a customer or transaction can be continually reevaluated based on new blockchain data). DASPs can combine KYT with traditional compliance tools to enhance their risk evaluation of customers associated with those transactions.

Whereas KYT is immediate, independent, and dynamic, traditional KYC is the opposite. It is based on financial institutions collecting static data points about a customer at the time of account opening, such as identification documents, account statements,

---

[52] *See* Ari Redbord, et al., *Home Alone? Never, with Transaction Monitoring*, (Sept. 22, 2022), https://www.acamstoday.org/home-alone-never-with-transaction-monitoring/ (emphasizing how "the blockchain allows for unprecedented visibility on financial flows."); Michael Morell, et al., *An Analysis of Bitcoin's Use in Illicit Finance* 5 (Apr. 6, 2021), https://cryptoforinnovation.org/wp-content/uploads/2022/07/An-Analysis-of-Bitcoins-Use-in-Illicit-Finance-By-Michael-Morell.pdf ("A currently serving official at the [Commodity Futures Trading Commission] added that it 'is easier for law enforcement to trace illicit activity using Bitcoin than it is to trace cross-border illegal activity using traditional banking transactions, and far easier than cash transactions.'").

[53] *See* Jai Ramaswamy, *How I Learned to Stop Worrying and Love Unhosted Wallet: Former DOJ AML Chief Considers the Unintended Consequences of Unhosted Wallet Transactions and the Regulatory Benefits of Cryptocurrency Adoption*, (Nov. 18, 2020), https://www.coincenter.org/how-i-learned-to-stop-worrying-and-love-unhosted-wallets/; see also Neal B. Christiansen and Julia E. Jarrett, *Forfeiting Cryptocurrency: Decrypting the Challenges of a Modern Asset*, 67(3) Department of Justice Journal of Federal Law and Practice 155, 166 (Sept. 2019) ("Cryptocurrency, despite the purported anonymity it grants criminals, provides law enforcement with an exceptional tracing tool: the blockchain.").

[54] *See* FATF, Updated Guidance for a Risk-Based Approach to VAs and VASPs 234 (Oct. 2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf (noting that "[b]lockchain analytics are … widely used by VASPs … to monitor their own exposure to risk.").

corporate records - and typically only occasionally refreshing those data points. Further, KYC is resource-intensive because it requires compliance professionals to manually collect and review documentation, consuming compliance resources that could be used on other, higher-impact activities, such as conducting SAR investigations. By contrast, KYT allows compliance resources to be deployed in a more targeted and effective manner, for example by generating alerts of suspicious transactions that warrant additional scrutiny.

In the following ways, DASPs have incorporated blockchain analytics and KYT into many key areas of compliance programs, including transaction monitoring, customer risk ratings, and sanctions controls.

- *First*, KYT can be directly incorporated into transaction monitoring tools so that a DASP can be alerted when a customer engages in risky transactions, both on and off its platform - which includes transactions with both hosted and self-hosted wallets.[55] Alerts can be based on numerous factors, such as transactions indicative of money laundering, contacts with high-risk actors and platforms, and other bespoke indicators.[56] When an alert is triggered, DASPs can then carry out additional diligence on the customer, prevent a transaction, investigate for potential SAR filing, or take other measures.

- *Second*, DASPs can incorporate KYT into a customer's risk rating. While initial risk ratings based on KYC information are static because the information is collected at the time of account opening, KYT data (which leverages the blockchain) can be used to inform the overall customer's risk rating as part of ongoing monitoring, and can act as a trigger for a DASP to take further action, such as conducting enhanced diligence reviews, closing the account, or filing a SAR.

- *Third*, blockchain analytics also augments sanctions compliance efforts in which DASPs directly screen for crypto addresses identified by economic sanctions regulators - such as Treasury's Office of Foreign Assets Control ("**OFAC**") - and can then proactively build out larger networks of high-risk addresses. Before the

[55] *See, e.g.*, Chainalysis, *How Chainalysis Helps Compliance Teams Address Sanctions Red Flags* (Mar. 8, 2022), https://blog.chainalysis.com/reports/fincen-russia-sanctions-red-flags-chainalysis/ (describing how blockchain analytics tools can be customized, allowing compliance teams to "assign unique transaction thresholds for alerts to be triggered for different counterparty categories based on their own risk strategy."). For reference, wallets where user funds are controlled by third parties, such as financial institutions, are called "hosted" wallets, whereas "wallets where users control the funds" are called "self-hosted" or "unhosted" wallets. See U.S. Dep't of the Treasury, *supra* note 2, at 15.

[56] *See* Chainalysis, *supra* note 55 (noting that "compliance teams can set customized alerts to be notified immediately when customers transact with mixing services above a specific threshold of their choosing.").

advent of crypto, OFAC was limited to putting static, traditional identifiers (like names and addresses) on its Specially Designated Nationals ("**SDN**") List. But with blockchain technology, sanctions compliance can now be based on transactional data, not just PII. With blockchain analytics, DASPs can take ground-truth addresses provided by OFAC to build out and identify much larger networks of high-risk counterparties using blockchain heuristics. From a relatively small number of blockchain addresses identified by OFAC, DASPs can build out large networks of addresses that they do not allow customers to transact with. And they can do this by leveraging immutable transactional data on the blockchain that is unrestricted by private ledgers and can tell them about common ownership. Traditional identifiers also result in high false positive rates, increasing the cost of compliance. With blockchain technology, false positives have been nearly eliminated.

In assessing efforts to combat illicit finance, Treasury already recognizes the powerful tools that blockchain technology and digital assets offer for promoting compliance. This consultation recognizes that "many digital assets operate on public blockchains," and the U.S. government itself "leverages public blockchain data and blockchain analytics to trace and attribute illicit activity in digital assets."[57] AI holds the promise to make efficient use of this information, while blockchain can protect against some of the key risks and concerns around privacy, interoperability, standardization, and protection.[58]

Case Examples: Integration of Blockchain Into AML

While AML and sanctions compliance teams at DASPs, along with other investigators, regularly use blockchain tools to successfully combat illicit finance, there have been several noteworthy examples in recent years of these tools' power, including those described below.

Fighting the use of crypto in terrorist financing

While terrorist financiers are more likely to abuse traditional financial assets than digital assets,[59] investigators have identified examples of terrorist groups and their financial

[57] U.S. Dep't of the Treasury, *Innovative Methods To Detect Illicit Activity Involving Digital Assets*; *Request for Comment*, 90 Fed. Reg. 40148 (Aug. 18, 2025).
[58] Coinbase Institute, *supra* note 27.
[59] U.S. Dep't of the Treasury, *2022 National Terrorist Financing Risk Assessment*, 21–22 (Mar. 1, 2022) https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf. Indeed, in 2020 illicit activity represented less than 1% of all activity in the cryptocurrency space - and of that, less than 0.05% of all illicit cryptocurrency transactions were associated with terrorist financing. Heidi Wilder, *An Overview of the Use of Cryptocurrencies in Terrorist Financing*

supporters soliciting or otherwise using crypto.[60] Advanced blockchain analytics tools have been critical to these investigations.

For instance, the Special Investigations team at Coinbase has reported on its research of blockchain records to assess terrorist organizations' fundraising efforts.[61] Among other things, they determined that, at the time of their report, Hamas had raised far more funds than other terrorist organizations (such as Al Qaeda and ISIS), in part because Hamas was actively soliciting bitcoin donations through its website and related social media channels.[62] Blockchain data further revealed how long Hamas had been soliciting bitcoin donations, the group's efforts to obfuscate its fundraising efforts by creating fresh donation addresses, and that Hamas has increasingly turned to other kinds of cryptocurrencies, such as Ethereum, to fund its efforts.[63]

Thanks to these blockchain analytics and other advanced tools, Coinbase was able to prevent its users from sending funds to organizations associated with these addresses, detect wider terrorism-financing efforts (identifying possible participants and accessories), and coordinate with law enforcement and regulatory agencies.[64] Of note, in April 2023 Hamas announced that it would stop using bitcoin for fundraising, citing increased efforts to prevent people from sending bitcoin to the organization.[65] More recently, the Iranian Islamic Revolutionary Guard Corps has been attributed to on-chain fundraising.[66] In response, Coinbase is taking similar measures to leverage blockchain analytics to detect additional addresses and participants in order to prevent transactions with these parties and to aid in counter terrorist financing efforts.

Promoting Sanctions Compliance with Blockchain Technology

Ordinary fiat currency laundered through traditional financial institutions remains a

---

(Sep. 21, 2021), https://www.coinbase.com/blog/an-overview-of-the-use-of-cryptocurrencies-in-terrorist-financing.

[60] U.S. Dep't of the Treasury, *supra* note 59 at 22 (describing U.S. law enforcement's review of domestic and international terrorist group's efforts to use cryptocurrency).

[61] Wilder, *supra* note 59.

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] Nidal Al-Mughrabi, *Hamas Armed Wing Announces Suspension of Bitcoin Fundraising*, April 28, 2023, https://www.reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28/ (explaining further how "developments in technology that track the movement of crypto on the blockchain ledger have made it easier for authorities to identify those behind crypto transfers.").

[66] U.S. Dep't of the Treasury, Press Release, *Treasury Targets Financial Network Supporting Iran's Military* (Sept. 16, 2025), https://home.treasury.gov/news/press-releases/sb0248

significant mechanism for sanctions evasion. For instance, Treasury has noted that, with regards to U.S. sanctions against Iran, the "Iranian regime has long used front and shell companies to exploit financial systems around the world" to evade sanctions.[67] By leveraging opaque ownership structures, incorporating in known tax havens, and using other laundering techniques involving fiat assets, bad actors make it difficult to follow the complex financial trails they leave behind.[68]

By contrast, crypto transactions are traceable, permanent, and public - enabling "sophisticated blockchain analytics programs to identify high-risk behavior, study emerging threats, and develop new mitigations."[69] In one such example, following Russia's invasion of Ukraine in 2022, Coinbase – in concert with traditional AML measures, such as using KYC information to block persons in sanctioned countries from opening an account – was able to use blockchain analytics to proactively identify and blocks tens of thousands of crypto addresses held by sanctioned individuals and/or Russian individuals and entities believed to be engaged in illicit activity.[70] Further, Coinbase was able to share those addresses with government officials to further support sanctions enforcement efforts.[71]

Welcome to Video

In October 2019, DOJ announced the takedown of Welcome to Video ("**WTV**"), the largest child sexual exploitation market in the world.[72] WTV made thousands of videos available for download to its members - and boasted of over one million downloads – in exchange for bitcoin. Fortunately, due to the online trail of funds this created, investigators were able to use advanced blockchain analysis to trace transactions to and from WTV's administrator, as well as many of its users and contributors.[73] Further analysis indicated

---

[67] Financial Crimes Enforcement Network, *Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System* (Oct. 11, 2018), https://www.fincen.gov/sites/default/files/advisory/2018-10-12/Iran%20Advisory%20FINAL%20508.pdf.
[68] Paul Grewal, *Using Crypto Tech to Promote Sanctions Compliance* (Mar. 6, 2022) https://www.coinbase.com/blog/using-crypto-tech-to-promote-sanctions-compliance.
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] Press Release, U.S. Dep't of Justice, *South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin* (Oct. 16, 2019), https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child.
[73] Chainalysis, *How Blockchain Analysis Helped take down the Largest Child Sexual Abuse Material Site* (Oct. 19, 2019), https://go.chainalysis.com/rs/503-FAP-074/images/Welcome%20to%20Video%20Case%20Study%20-%20FINAL.pdf.

that some of these individuals were utilizing addresses at KYC-compliant exchanges, which enabled law enforcement to gather additional information about – and ultimately identify, arrest, and prosecute – hundreds of individuals associated with WTV.[74]

Twitter Hack

In July 2020, the Twitter accounts of a number of high-profile individuals, including Bill Gates and Barack Obama, were compromised to post a "double your bitcoin" crypto investment scam.[75] The actors who compromised the accounts used their access to post messages on Twitter directing victims to send crypto to various bitcoin addresses.[76] For example, a message posted on Bill Gates's Twitter account stated, "I am doubling all payments sent to my [bitcoin] address for the next 30 minutes. You send me $1,000, I send you back $2,000."[77] As a result, the scam bitcoin accounts received more than 400 transfers worth more than $100,000.[78] Of course, no bitcoin was returned.[79] Fortunately, law enforcement officials - in part through data obtained from Coinbase about the bitcoin addresses involved in the hacks - were able to track the identities of the hackers,[80] leading to their arrest and prosecution.[81]

Regulatory Obstacles and Recommendations

Developments to the U.S. regulatory regime with respect to utilizing blockchain technology should follow a functional, risk-based approach that reinforces and modernizes the existing framework.

Supporting law enforcement with the tools they need

As an initial matter, we recommend that policymakers ensure that law enforcement is well equipped to develop local-state-federal task forces to share information and combat

---

[74] *Id.*
[75] *See* Sheera Frenkel, et al., *A Brazen Online Attack Targets V.I.P. Twitter Users in a Bitcoin Scam*, N.Y. Times, July 15, 2020, https://www.nytimes.com/2020/07/15/technology/twitter-hack-bill-gates-elon-musk.html.
[76] Criminal Complaint ¶ 21, *United States v. Fazeli* (July 31, 2020), https://www.justice.gov/d9/press-releases/attachments/2020/07/31/fazeli_complaint_0.pdf ("Fazeli Complaint").
[77] Catalin Cimpanu, *How the FBI Tracked down the Twitter Hackers*, ZDNET, July 31, 2020, https://www.zdnet.com/article/how-the-fbi-tracked-down-the-twitter-hackers/ ("Twitter Hackers").
[78] Press Release, U.S. Dept. of Justice, *Three Individuals Charged For Alleged Roles In Twitter Hack* (July 31, 2020), https://www.justice.gov/usao-ndca/pr/three-individuals-charged-alleged-roles-twitter-hack ("DOJ Twitter Press Release").
[79] Fazeli Complaint ¶ 29.
[80] Twitter Hackers; Fazeli Complaint ¶ 51.
[81] DOJ Twitter Press Release, *supra note 78*.

illegal activity. Treasury should also support international partnerships to help combat efforts by unregulated international entities who move crypto in a manner that facilitates illegal activity. Despite the incredible proliferation of crypto investigation expertise throughout law enforcement agencies over the last several years, there are often situations where law enforcement, especially at the local level, lacks the tools and resources necessary to pursue crypto-related crime. This is especially true in large-scale cases where victims may be located across the country, or in cases where the criminals are based overseas. Resources from Congress would help close this gap.

Support of new, enhanced blockchain tools

Congress intended to support regulatory and law enforcement use of new, enhanced blockchain tools when it passed AMLA, encouraging technological innovation and the adoption of new technology to more effectively counter illicit finance.[82] Legislation should actively promote the use of blockchain technology for compliance by creating a clear and supportive regulatory environment for "RegTech" innovation. Another avenue for regulatory support of blockchain analytics is the use of OFAC licenses for blockchain analytics providers to engage with sanctioned entities in order to develop more fulsome repositories of addresses controlled by those entities. To counter the associated risk that DASPs would be forced to maintain contracts with such analytics providers in order to access this data, we would also recommend that analytics providers share lists of these addresses more broadly with the digital asset industry. Alternatively, OFAC could require analytics providers granted these licenses to share their findings with OFAC, which could then submit the data to a multi-agency review process to determine whether to officially designate additional wallet addresses as SDNs.

[82] Div. F of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, Div. F, 134 Stat. 3388, 4547 (2021).

Recognize risk-based use of KYT and clustering

Treasury should publish supervisory guidance that explicitly recognizes blockchain analytics, KYT outputs, and clustering as acceptable, risk-based evidence in AML and sanctions programs. The guidance should outline evidence "tiers" (i.e. ground-truth designations, platform verified labels, open-source intelligence, commercial tool inferences) and when each tier supports blocking, monitoring, investigation, etc., along with mandatory confidence scoring and recordkeeping for the underlying logic. This reflects the practical reality that blockchain attribution is probabilistic and corroboration-driven, and that multiple institutions may legitimately disagree on classifications.

Continued information sharing and coordination

Legislation and agency policies should be updated to encourage sharing information relevant to potential illicit activities routed through blockchains. Agencies should publish information – such as addresses, services, and clusters – in API feeds, designations and advisories, and publish typology playbooks that illustrate common obfuscation patterns, entity behaviors, and red-flag trends. This facilitates private sector tools to grow sanctions networks from a small seed into much larger interdiction sets.

Applying the BSA in a technology-neutral manner

To ensure strong consumer protection while preserving space for innovation, the definition of a "financial institution" under the BSA should be applied in a technology-neutral and functional manner. It should encompass participants that perform the core functions of a financial intermediary, namely those who exercise total independent control of customer assets, mirroring the framework that FinCEN has already established. This would include centralized exchanges, custodians, and other custodial wallet providers. Crucially, just as was done in the GENIUS Act definition of "Digital Asset Service Provider" – which specifically excludes validators, non-custodial software interfaces, and distributed ledger protocols – the definition should not be extended to participants who do not perform these functions. This exclusion should explicitly cover non-custodial software developers, hardware wallet manufacturers, node operators who merely validate or sequence transactions, and individuals or entities engaged in staking to secure a network without acting as a service provider for others. Much like a cloud services provider or a telecommunications company would secure their own networks, these non-custodial service providers cannot see PII for individual transactions – nor should we want them to do so. Protecting the privacy of Americans has long been a goal of Congress, but imposing BSA-like requirements on non-custodians would put all Americans at risk.

By way of example: blockchain validators are typically decentralized by design, meaning that, if they were required to collect PII, that PII would exist in many, many places – creating numerous "honeypots" for cybercriminals to target. This risk would further be exacerbated by the BSA's requirement to retain data for years. We therefore strongly recommend that policymakers reinforce the existing regulatory framework that, for decades, has guided consumers and industry, instead of imposing unworkable and counterproductive compliance burdens on those who are merely building or maintaining the infrastructure of the crypto ecosystem but do not touch customers' funds.

This does not mean that the exchange of funds via non-custodial channels and tools should be unregulated. To the contrary – it should be tightly regulated through the access points that enable the underlying transfer of value. As noted above, these on- and off-ramps are necessary to cash out. Those should be (and in the U.S., already are) regulated. Further, end-users of non-custodial products should face consequences for their illegal activity; just like with cash, if a crime occurs as a result of a user's action, the perpetrators should face justice.

This same logic applies to digital asset mixers and tumblers, where policymakers' focus should be on the illicit use of these tools, not on banning the technology itself. Privacy-enhancing technologies have legitimate applications and are a crucial area of innovation. An outright ban would be ineffective, as these protocols are often open-source and decentralized, thereby harming law-abiding users seeking privacy. Instead, policy should focus on strengthening the ability of law enforcement and regulators to trace illicit funds into and out of mixers using advanced on-chain analytics. Enforcement actions should target those who knowingly facilitate money laundering through these tools – as well as the exchanges that flout their AML/KYC obligations, creating a tempting off-ramp where bad actors flock to cash out. This balanced approach preserves the ability of developers to write and publish code (a form of speech) and for individuals to maintain privacy in their personal financial affairs, while ensuring that the points of greatest systemic risk have proper oversight.

Finally, the President's authority under the International Emergency Economic Powers Act ("**IEEPA**") should apply to digital assets to the same extent it applies to any other form of property in which a foreign national or country has an interest. Digital assets are property, and the existing authority is sufficient to allow the President to block transactions and freeze assets to address threats to national security, foreign policy, or the economy. The application of IEEPA should continue to be implemented by OFAC through its sanctions programs, which can and do target specific digital asset addresses associated with sanctioned individuals, entities, or regimes. No expansion of the fundamental authority is necessary; rather, continued investment in the technical capability to enforce that authority in the digital asset domain is required.

GENIUS Act Research Factors

We set forth below ways use of blockchain technology relates to and impacts certain research factors Congress identified in the GENIUS Act.

- **Improving Detection of Illicit Activity -** Blockchain technology unlocks greater effectiveness in combating illicit financial activity than rules-only screening and analysis. KYT and on-chain clustering broaden the aperture beyond static PII lists by leveraging immutable transaction records. Institutions can expand to much larger networks they can monitor, yielding faster interdiction, better internal risk profiling, and richer SARs. Law enforcement casework demonstrates that on-chain visibility reveals supply chains, not just endpoints.

- **Costs to Financial Institutions** - Up-front costs of such programs include data ingestion/engineering, specialized investigators, tooling, and model-risk governance. However, financial institutions report offsetting savings from better alert quality (fewer false positives), quicker triage, and reusable investigative artifacts that scale across cases. Clear regulatory expectation reduces interpretation "tax," letting teams invest in durable controls instead of one-off justifications.

- **Data Scope & Privacy Risks** - The data "collected" and reviewed is public blockchain data. Robust analysis of blockchain ledgers enables AML programs to minimize PII collection by emphasizing objective, on-chain signals. The right safeguards (e.g., confidence scoring, human-in-the-loop reviews, audit logs, and clear retention limits) protect against overcollecting identity data. Where identity is needed, decentralized credentials like ZK Proofs and selective-disclosure proofs can satisfy reliance requirements while keeping sensitive documents out of routine flows, lowering breach risk and consumer friction.

- **Operational Efficiency** - For sanctions screening, when analytics vendors integrate into case management, sanctions engines, and payment controls, financial institutions can screen and interdict nearly in real time rather than wait for manual escalations.

- **Cybersecurity -** Graph labels and watchlists are sensitive and should be protected like other high-impact data. Programs need secure ingestion, change-control, and strong vendor risk management. Agencies can reinforce this by mapping expectations to established controls and by funding law-enforcement training and tools. Because public chains are transparent, attackers often pivot to weaker off-ramps and non-compliant venues. This reinforces the pairing of strong cybersecurity with targeted enforcement.

- **Overall effectiveness -** Combining KYC with on-chain, shareable transaction data is a compliance multiplier. Financial institutions see farther, act faster, and coordinate better. The result is materially improved prevention, detection, and recovery compared to legacy tools alone.

VII. Conclusion

The emergence of cryptocurrency has provided an unprecedented opportunity to combat illicit finance using tools that harness the public and transparent nature of the blockchain, as well as other innovative tools like AI, DiD, and APIs. As the case examples discussed above show, DASPs are already implementing these tools to more effectively prevent money laundering and terrorist financing, among other financial crimes, from happening on their platforms.

Moreover, all of these tools go hand-in-hand to streamline processes and reduce compliance burdens. Adoption of DiDs to reduce or remove CIP/KYC obligations, together with AI and Machine Learning improvements to transaction monitoring and sanctions controls – driven by blockchain analytics efficiencies – can reduce superfluous alerts, investigations, and SAR filings. This will result in greater focus by both DASPs and regulators on the emerging, high-risk threats to the financial system.

Regulators can better support the fight against illicit finance by focusing on certain industry participants' non-compliance with existing regulations, ensuring consistent enforcement efforts, and supporting the adoption of decentralized identity tools. In turn, industry should be willing to work with governments to develop sound, constructive regulations. By encouraging novel and collaborative approaches to combating illicit finance, regulators can make regulatory and law enforcement efforts more effective while not deterring new innovations in financial services.