coinbase

Coinbase, Inc.
248 3rd St Box 434
Oakland, CA 94607

August 31, 2023

European Banking Authority
Tour Europlaza
20 avenue André Prothin
CS 30154
92927 Paris La Défense CEDEX
France

Sent via EBA online response portal:
https://www.eba.europa.eu/consultation-revised-guidelines-money-laundering-and-terrorist-financing-mltf-risk-factors-form

RE: Response to the EBA Consultation on Revised Money Laundering and Terrorist Financing (ML/TF) Risk Factors

To Whom it May Concern:

Coinbase Inc. ("Coinbase") is providing the following response to the European Banking Authority's ("EBA") Consultation on the Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risks associated with individual relationships and occasional transactions (the "Guidelines") under Articles 17 and 18(4) of Directive (EU) 2015/849.

Our comments relate to proposed Guideline 21, specifically **Guidelines 21.3(d)(i) and 21.5(b)(xv)(b).**

Guidelines 21.3(d)(i) and 21.5(xv)(b) categorize transactions involving self-hosted wallets (SWHs) as a factor that firms may consider as contributing to an increased risk.

For the reasons set forth below, we assert that it is incorrect to categorize all transactions with self-hosted wallets as high-risk.

To the extent there may be potential illicit finance risks associated with SHWs, those risks are adequately addressed by the existing anti-money laundering ("AML") requirements on regulated CASPs. Not only are CASPs able to use their advanced suite of compliance tools to identify potentially risky counterparties (*see* Appendix A at pp. 2-6), they are also already obligated to carry out traditional compliance measures on those transactions, such as filing STRs, risk rating customers transacting with those wallets, and carrying out additional diligence when warranted. CASPs can use advanced compliance tools, such as know-your-transaction (KYT) to precisely and dynamically understand the risk posed by a counterparty in a crypto transaction based on verifiable and independent data, including when the counterparty is a SHW (*see* Appendix A at p. 4). This applies even if customers are

sending to multiple addresses, as advanced analytic tools used by CASPs are able to connect multiple transactions associated with a single originator or beneficiary.

Moreover, the Guidance should be based on actual risk, not concerns about potential illicit activity. For instance, SHWs do not present a significant illicit finance risk and thus should not be considered categorically high risk. The Financial Action Task Force ("FATF"), the international body tasked with analyzing illicit finance and setting global AML standards, carried out an extensive study on SHWs and was unable to identify them as categorically high risk.[1] Even more, the UK Treasury in a recent report found that "there is not good evidence that [SHWs] present a disproportionate risk of being used in illicit finance," and further acknowledged that "many persons who hold [crypto] for legitimate purposes use [SHWs] due to their customisability and potential security advantages."[2]

Rather than posing a heightened risk, SHWs are an important and healthy part of the crypto ecosystem. Just like web browsers have given consumers broad access to the Internet, SHWs are doing the same for crypto markets. Consumers depend on SHWs to securely store crypto assets, directly engage with decentralized applications that provide a wide array of services, and create verified identities (known as "digital identity"). Additionally, SHWs provide for personal security, as users can store their assets digitally without the risks of holding physical assets like cash or gold.

This is a powerful advantage for the unbanked, who would otherwise be forced to physically store their personal assets—a particular concern for those living in high crime areas or needing to transfer value to family in other parts of the world. Further, SHWs are the core technology for a new wave of web applications built on the blockchain (collectively referred to as "Web3"[3]), that allow users to control their own data when interacting with centralized software providers—thus reducing the ability of third parties to collect and store large troves of personal identifying information. In the future, SHWs will act as the gateway to Web3.

* * *

[1] See Financial Action Task Force, *Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* ¶¶ 119–20 (July 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf ("FATF July 2021 Report") (acknowledging that "the size of the [peer-to-peer] sector and its associated [AML] risk remains unclear," and that "given the strong evidence of the risks posed by deficient or non-compliant [CASPs], the FATF's focus on placing [AML] controls on intermediaries (such as [CASPs]) should be maintained for the time being"); see also FATF October 2021 Guidance ¶ 296 (noting merely that transactions with SHWs "may be attractive to illicit actors," and advising CASPs to employ "the appropriate risk-based controls") (emphasis added).

[2] HM Treasury, *Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Statutory Instrument 2022: Response to the Consultation*, Chap. 6.21 (June 2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1083351/MLRs_SI_2022_-_Consultation_Response_final.pdf.

[3] *See* Ethereum.org, *Introduction to Web3*, https://ethereum.org/en/web3/ (outlining the strengths of Web3 as a decentralized, permissionless, and trustless system that empowers individual users).

<u>We encourage the EBA to modify it's Guidance as follows</u>:

21.3(d)(i): Instead of categorizing all "self-hosted addresses" as high risk, the language should be modified to: "*self-hosted addresses associated with higher risk of illicit activity.*"

21.5(b)(xv)(b): Instead of categorizing all transactions involving "multiple self-hosted addresses or multiple addresses located in other CASP" as high risk, the language should be modified to: "*multiple self-hosted addresses or multiple addresses located in other CASP associated with higher risk of illicit activity.*"

We thank you for this opportunity to respond to the proposed amendments to the Guidelines and welcome the opportunity to discuss this issue further with the EBA.

Sincerely,

Grant Rabenn
Director - Financial Crimes Legal
Coinbase
grant.rabenn@coinbase.com

APPENDIX A

coinbase

November 1, 2022

United States Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

Submitted electronically via regulations.gov

Re: Ensuring Responsible Development of Digital Assets; Request for Comment

Coinbase Global, Inc. (Coinbase) welcomes the opportunity to respond to the U.S. Treasury Department's request for comment on "Ensuring Responsible Development of Digital Assets" (the RFC).[1] As a leader in the cryptocurrency ecosystem, Coinbase fully supports effective regulation developed with the input and coordination of industry members. This RFC comes at a time of enormous opportunity for the United States to lead the world in digital asset innovation, but this opportunity depends in significant part on Treasury and other key federal agencies creating a regulatory landscape that fosters the growth of compliant companies while holding accountable those that fail to meet their obligations.

In this response, Coinbase explains why the unique compliance opportunities provided by the blockchain enable far more effective disruption of illicit finance and compliance with anti-money laundering (AML) regulations, such that Treasury's focus should not be on adding new regulatory requirements. Rather, Coinbase recommends that Treasury prioritize the enforcement of existing, robust AML regulations against noncompliant market participants, while working with the crypto industry to unlock groundbreaking new compliance technologies—including in the areas of blockchain analytics and decentralized identity—and developing a federal framework for payments regulation.

This comment letter is divided into three parts.

First, we describe how virtual asset service providers (VASPs) comply with the existing regulatory regime, including how they leverage the exceptional compliance advantages of the blockchain that are more comprehensive, dynamic, and effective than those available to traditional financial institutions.

---

[1] U.S. Dep't of the Treasury, *Ensuring Responsible Development of Digital Assets; Request for Comment*, TREAS-DO-2022-0018-0001, 87 FR 57556 (Sept. 20, 2022), https://www.federalregister.gov/d/2022-20279.

Second, we describe how it is *noncompliance*—as opposed to any gaps in existing regulations—that poses the greatest illicit finance risk in crypto, and how Treasury can use its existing authority to address any failures to comply with existing AML regulations.

Third, we identify areas where Treasury can collaborate with industry stakeholders to enable the adoption of the next generation of compliance tools to further enhance effectiveness (such as digital identity technologies), and we describe our support for a federal framework for payments regulation.

I. Innovative, Blockchain-Based Compliance Technologies Provide an Unprecedented Opportunity to More Effectively Safeguard Against Illicit Finance than Traditional AML Controls Alone[2]

The Bank Secrecy Act (BSA) requires financial institutions to implement effective AML programs,[3] which include collecting know-your-customer (KYC) information; monitoring incoming and outgoing transactions; filing Suspicious Activity Reports (SARs); appointing a BSA officer; and training employees on compliance requirements. These requirements apply equally to Coinbase and other VASPs.

But the emergence of crypto over the last decade has given VASPs a powerful *new* set of compliance tools to radically enhance our effectiveness at identifying and disrupting illicit finance. These new tools harness the public and transparent nature of the blockchain, allowing VASPs 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—in other words, "Compliance 3.0."[4]

---

[2] This section responds to the RFC's general request for input, as well as the following questions in the RFC: B1, B3, B4, D1, D2, D4, D5, and D7.

[3] *See, e.g.*, 31 CFR § 1022.210(a) (requiring money services businesses to have "[a]n effective anti-money laundering program … that is reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities.").

[4] Compliance 1.0 was the use of paper documents and manual review of accounts throughout the first few decades after the BSA was passed in 1970. Compliance 2.0 emerged in the 2000s when financial institutions began incorporating software into their compliance controls. Compliance 3.0 is the next generation of compliance tools based on blockchain data and software, which give financial institutions unprecedented visibility into activity on and off their platforms. *See* Dmytro Foremnyi, *Compliance 3.0: where are we heading?* (Nov. 29, 2018), https://complianceperiscope.com/home/2018/11/29/compliance-30-where-are-we-heading.

In the world of Compliance 3.0—where VASPs are leveraging enhanced compliance technologies to dynamically assess risk—Treasury should focus on incentivizing and increasing adoption of new technologies to further increase effectiveness, as opposed to imposing new, ineffective bulk data collection/reporting requirements.

A. To Comply with Existing AML Regulations, VASPs Are Not Limited to Relying on Traditional Controls but Can Leverage the Transparency of the Blockchain to Deploy New Technologies that Substantially Enhance the Effectiveness of their Compliance Programs

To meet their BSA obligations, VASPs like Coinbase have devoted enormous resources to developing effective compliance programs. This includes traditional controls like collecting KYC information, monitoring on-platform transactions, and filing SARs, but more critically, deploying innovative technologies that leverage the public and transparent nature of the blockchain, which is not constrained by private ledgers.

Blockchains collect all transactions and record them on a common, public ledger. This means that VASPs (along with regulators and law enforcement) can analyze transactions carried out on that blockchain—whether or not they took place on the VASP's own platform.[5] In contrast, a traditional financial institution is largely limited to using private, opaque ledgers that are only available to that specific institution. This creates significant risk of blind spots for traditional financial institutions because it is difficult—if not impossible—for them to fully monitor transactions that happen off of their individual platforms. 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 analyze the full history of those funds. Crypto fixes this problem by giving VASPs unprecedented access to the full scope of transactional records.[6]

---

[5] *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.'").

[6] *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),

This additional data (not limited by private ledgers) lets VASPs 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 know-your-transaction (KYT). An entire industry of blockchain analytics firms have developed in recent years to assist VASPs and law enforcement in utilizing the treasure-trove of data held in blockchains.[7] 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),[8] and *dynamic* (the risk associated with a customer or transaction can be continually reevaluated based on new blockchain data). VASPs can then combine KYT with traditional compliance tools to enhance their risk ratings 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, corporate records—and typically only occasionally refreshing those data points. Further, KYC is resource-intensive to carry out 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.

---

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.").

[7] *See* Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* ¶ 234 (Oct. 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf ("FATF October 2021 Guidance") (noting that "[b]lockchain analytics are … widely used by VASPs … to monitor their own exposure to risk.").

[8] *See* Robert Werner, et al., *Blockchain Analysis Tool of Cryptocurrency*, ICBCT '20: Proceedings of the 2020 The 2nd International Conference on Blockchain Technology 80 (Mar. 2020), https://dl.acm.org/doi/pdf/10.1145/3390566.3391671 ("The blockchain … is an immutable ledger, which is stored on a large network of servers worldwide in a decentralized manner. On this ledger, all transactions are stored permanently, transparently and can be accessed by anyone.").

In the following ways, VASPs have incorporated 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 VASP 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.[9] 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.[10] When an alert is triggered, VASPs can then carry out additional diligence on the customer, investigate for potential SAR filing, or take other measures.

Second, VASPs can dynamically 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 dynamically added to a customer's risk rating. If the rating rises to a certain level, VASPs can take further action, such as conducting enhanced diligence reviews, closing the account, or filing a SAR.

Third, KYT also creates an enhanced approach to sanctions compliance in which VASPs directly screen for crypto addresses identified by the Office of Foreign Assets Control (OFAC) and can then proactively build out larger networks of high-risk addresses. Before the advent of crypto, OFAC was limited to putting static, traditional identifiers—such as 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 personal identifying information (PII). With blockchain analytics, VASPs 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, VASPs 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.

---

[9] *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.").

[10] *See id.* (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.").

These new, enhanced compliance technologies are exactly what Congress envisioned when it passed the Anti-Money Laundering Act of 2020 (AMLA).[11] A key goal of AMLA was to "encourage technological innovation and the adoption of new technology … to more effectively counter" illicit finance.[12] And as Congress described, the AMLA "provides a clear *mandate for innovation*" and for financial institutions to "*effectively* ... test, and adopt leading technologies ... to track, identify, and report suspicious financial activity."[13] Congress deemed this reform important, contrasting the "decades-old regime … built on individual reporting requirements (i.e., currency transactions reports (CTRs)" with "the current, sophisticated AML compliance systems now managed by most financial institutions."[14] To that end, the AMLA calls upon Treasury to help revitalize the AML compliance landscape by, among other things, issuing a rule specifying standards for testing BSA-compliance technology and internal processes, including transaction-monitoring systems.[15] It also establishes a new "tech symposium," where Treasury can talk with private industry about the implementation of emerging technologies intended to prevent illicit activity, including "digital identity technologies, distributed ledger technologies, and other innovative technologies."[16] Treasury has a great opportunity to carry out AMLA's mandate by encouraging the widespread adoption of KYT and similarly cutting-edge tools to truly enhance effectiveness.

---

[11] The AMLA is contained in 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).

[12] AMLA § 6002.

[13] United States. Congress. Joint Explanatory Statement of the Committee of Conference on H.R. 6395, at 732 https://docs.house.gov/billsthisweek/20201207/116hrpt617-JointExplanatoryStatement.pdf (emphasis added).

[14] *Id.* at 731–32.

[15] *See* AMLA, § 6209. Similarly, the New York State Department of Financial Services (NYDFS), a significant regulator in the crypto space, has issued guidance encouraging firms to utilize blockchain analytics to fulfill AML obligations. NYDFS, *Guidance on the Use of Blockchain Analytics* (April 28, 2022), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20220428_guidance_use_blockchain_analytics.

[16] AMLA § 6211. *See also id.* § 6208 (establishing BSA Innovation Officers to advise stakeholders on innovative technologies); *id.* § 6210 (requiring Treasury to analyze the impact of new technologies on compliance).

B. Treasury Should Focus on Increasing Adoption of New Blockchain-Based Compliance Tools, Not Imposing Ineffective Bulk Data Collection Requirements

Treasury's proposal to require VASPs to bulk collect counterparty information on *all* transactions with self-hosted wallets over $3,000, and to file suspicionless CTRs on those greater than $10,000 (the Notice of Proposed Rulemaking, or "NPRM") runs counter to the goals of the AMLA to increase—not decrease—the effectiveness of AML programs. [17]

As an initial matter, regulations should be based on actual risk, not concerns about *potential* illicit activity. The Financial Action Task Force (FATF), the international body tasked with analyzing illicit finance and setting global AML standards, carried out an extensive study on self-hosted wallets and was unable to identify them as *categorically* high risk.[18] Nor did the NPRM cite any quantitative data showing so.[19] Even more, the UK Treasury in a recent report found that "there is not good evidence that self-hosted wallets present a disproportionate risk of being used in illicit finance."[20] Rather than posing a heightened risk, self-hosted wallets are an

---

[17] Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83840 (proposed Dec. 23, 2020) ("NPRM"), https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28437.pdf.

[18] *See* Financial Action Task Force, *Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* ¶¶ 119–20 (July 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf ("FATF July 2021 Report") (acknowledging that "the size of the [peer-to-peer] sector and its associated [AML] risk remains unclear," and that "given the strong evidence of the risks posed by deficient or non-compliant VASPs, the FATF's focus on placing [AML] controls on intermediaries (such as VASPs) should be maintained for the time being"); *see also* FATF October 2021 Guidance ¶ 296 (noting merely that transactions with self-hosted wallets "*may* be attractive to illicit actors" and advising VASPs to employ "the appropriate risk-based controls") (emphasis added).

[19] Instead, the NPRM, citing the FATF, speculates that peer-to-peer transactions potentially "*could* present a leak in tracing illicit flows of virtual assets." NPRM at 83,844 (emphasis added).

[20] HM Treasury, *Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Statutory Instrument 2022: Response to the Consultation*, Chap. 6.21 (June 2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1083351/MLRs_SI_2022_-_Consultation_Response_final.pdf (further noting that "unhosted wallets should [not] automatically be viewed as higher risk; many persons who hold [crypto] for legitimate purposes use unhosted wallets due to their customisability and potential security advantages.").

important and healthy part of the crypto ecosystem that allow users to directly participate in a new ecosystem of internet services built on blockchain technology, referred to as "Web3."[21]

Importantly, any potential illicit finance risk associated with self-hosted wallets is adequately addressed by the existing AML requirements on regulated VASPs. Not only are VASPs able to use their advanced suite of Compliance 3.0 tools to identify potentially risky self-hosted wallet counterparties, they are also *already* obligated to carry out traditional compliance measures on those transactions (described above), such as filing SARs, risk rating customers transacting with those wallets, and carrying out additional diligence when warranted. This is why the NPRM is unable to identify a regulatory gap preventing VASPs from being able to mitigate illicit finance risks posed by self-hosted wallets.[22]

The proposals in the NPRM are both unnecessary, but more critically, less effective than existing compliance solutions that leverage technology. As described above, VASPs can use KYT to precisely and dynamically understand the risk posed by a counterparty in a crypto transaction based on verifiable and independent data, even when the counterparty is a self-hosted wallet. Meanwhile, the bulk data collection proposed by the NPRM is exactly the opposite—*imprecise*, *static*, and *unverifiable*. This is because VASPs must rely on information provided by customers when collecting the counterparty's name and address. But customers may not be able to collect this information accurately from the counterparty, or, for entirely legitimate reasons, may have no direct relationship with the counterparty (such as if the counterparty is a merchant or a smart contract). Further, the VASP collecting this data will have no contractual terms of service with the counterparty, and will thus have no way of compelling the counterparty to verify the accuracy of the data. In this case, bad actors could simply provide false information about their counterparties, leaving VASPs with inaccurate data in their systems. And bad data coming into compliance systems will lead to bad data going out in the form of inaccurate SAR filings and data sharing pursuant to Section 314 of the USA PATRIOT ACT—a detrimental outcome for regulators and law enforcement.

It is also possible that, for entirely legitimate privacy reasons, customers not wanting to identify their counterparties will simply first send funds to their self-hosted wallets and then from there to the ultimate beneficiaries. This means that compliance teams and law enforcement would receive no additional information about the true counterparty, all while increasing the

---

[21] *See* Ethereum.org, *Introduction to Web3*, https://ethereum.org/en/web3/ (outlining the strengths of Web3 as a decentralized, permissionless, and trustless system that empowers individual users).

[22] NPRM at 83,844 (acknowledging that "hosted wallet providers are subject to the BSA" and are therefore required to undertake steps to mitigate financial crime risk, such as "conducting customer due diligence with respect to accountholders and reporting suspicious activity.").

administrative burden on VASPs that could otherwise be spent on more effective compliance activities. Even more, the NPRM's additional data-collection requirements would incentivize users to seek VASPs that fail to implement the requirement or operate in jurisdictions without this requirement, all of which would decrease U.S. law enforcement's visibility into illicit crypto actors and damage the overall health of the crypto ecosystem in the U.S.

Lastly, it would be unprecedented to require financial institutions to collect sensitive PII about non-customers, especially when not based on any suspicion of actual wrongdoing. This scenario creates a wide array of dangerous privacy risks not addressed in the NPRM, including opening up many crypto users to data hacks and other malicious cyber activities.[23]

In lieu of such proposals, Treasury should instead pursue more effective methods of safeguarding the financial system against illicit activities, including (as described above) by encouraging VASPs to leverage technology and the blockchain to more effectively combat illicit finance, such as through KYT, and by enforcing existing regulations against noncompliant actors, as described below.

II. Enforcing Existing Regulations is the Key to Combating Illicit Finance Risk in the Crypto Ecosystem[24]

Bad actors are often motivated by profit, seeing crypto as just another tool for making money. When they obtain crypto through criminal means, they typically choose to convert these funds to fiat currency to liquidate their proceeds. But in doing so, they generally seek to avoid using VASPs who meet their compliance obligations—who file SARs, require KYC information when onboarding customers, and can freeze illicit funds held in the criminal's account.[25] Instead, criminals flock to VASPs who fail to implement these controls to reduce their likelihood of

[23] As Coinbase previously cautioned in a response to the NPRM, "[c]reating a Treasury managed stockpile of name and address information tied to a public key on the blockchain presents real risks to privacy and safety and an even more attractive target for hackers." Coinbase, *Re: Docket No. FINCEN-2020-0020; RIN No. 1506-AB47*, at 2 (Jan 4, 2021), https://www.regulations.gov/comment/FINCEN-2020-0020-6205.

[24] This section responds to the RFC's general request for input, as well as the following questions in the RFC: B1 and B6.

[25] 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 ("DOJ Digital Assets Report") (cautioning 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 [AML] scrutiny.").

detection. But the U.S. government has the tools to address this illicit finance risk, because the Treasury has *existing* authority to enforce against noncompliant VASPs doing business in the U.S. or servicing U.S. customers in substantial part, whether or not these VASPs are physically located in the U.S.[26]

One of the most effective ways to combat illicit finance, therefore, is to disrupt the ability of noncompliant VASPs to liquidate and conceal criminal proceeds, which makes criminal behavior less profitable. The Treasury and the U.S. government more broadly already have ample authority in this regard, and adding additional regulatory obligations on compliant VASPs will not solve this illicit finance threat.

A. Criminals Rely on Noncompliant VASPs to Conceal and Monetize Their Illicit Activities

Treasury, FATF, and the U.S. Department of Justice (DOJ) have already highlighted the threat posed by noncompliant VASPs.[27] While a growing number of countries impose compliance obligations on VASPs, there are still large gaps in global enforcement efforts.[28] A number of VASPs 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.[29]

The evidence demonstrates that illicit actors—ransomware groups, sanctioned entities, darknet markets, scammers, and other cybercriminals—have sought out noncompliant VASPs to monetize their crimes.[30] This is no mystery, as criminals prefer VASPs they know require

---

[26] *See* 31 C.F.R. § 1010.100(ff); *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001, at 12 (May 9, 2019) ("FinCEN 2019 Guidance") (emphasizing that the BSA's "requirements apply equally to domestic and foreign-located [crypto] money transmitters doing business in whole or in substantial part within the United States, even if the foreign-located entity has no physical presence in the United States.").

[27] 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 (identifying "non-compliant VASPs used to launder or cash out illicit funds [as a] primary concern."); FATF July 2021 Report ¶ 73 (warning that illicit actors are taking advantage of poor screening processes at noncompliant VASP); DOJ Digital Assets Report at 7.

[28] *See* FATF July 2021 Report ¶¶ 26, 45.

[29] *See id.* ¶ 73.

[30] Chainalysis, *The 2021 Crypto Crime Report*, 9, 13, 74 (Feb. 16, 2021), https://go.chainalysis.com/2021-Crypto-Crime-Report.html (highlighting that "[cybercriminals] rely on a

minimal (if any) KYC information, won't restrict their customers from exchanging funds with illicit counterparties, and won't file SARs with government authorities.

B. Treasury Already Has Existing Authority to Hold Noncompliant Actors Accountable

Treasury can be a leader in enforcing existing regulations. Importantly, the Financial Crimes Enforcement Network (FinCEN) already has ample authority to independently investigate and bring enforcement actions against VASPs who violate the BSA, including civil money penalties.[31] Further, FinCEN may refer matters to law enforcement agencies for criminal prosecution, where the penalties against VASPs under federal criminal law are considerably more severe and may include lengthy prison terms. FinCEN has effectively wielded its authority in recent years, bringing enforcement actions against gatekeeper institutions for violating the BSA,[32] but it has brought very few actions against noncompliant VASPs for AML failures.

In failing to implement AML controls, noncompliant VASPs do not only attract criminals; they also attract some law-abiding customers who may simply want to avoid the hassle of providing KYC information that compliant VASPs are required to collect. This gives noncompliant VASPs a competitive edge for all the wrong reasons. The Treasury is uniquely positioned to use its existing authorities to ensure that all VASPs with ties to the U.S. are held to the same standards and to rout out illicit finance risks posed by this arbitrage. The U.S. government has much to gain by keeping the crypto industry onshore: regulators like Treasury can ensure compliance with AML regulations; law enforcement greatly benefits by being able to directly subpoena records from U.S. companies (as opposed to having to use cumbersome,

---

surprisingly small group of service providers to liquidate their crypto assets," including "money services businesses with lax compliance programs"); Elliptic, *Financial Crime Typologies in Cryptoassets: The Concise Guide for Compliance Leaders* 10 (2020) https://www.elliptic.co/hubfs/Financial%20Crime%20Typologies%20in%20Cryptoassets%20Guides%20(All%20Assets)/Typologies_Concise%20Guide_12-20.pdf ("Criminals deliberately seek out exchanges they know they can exploit with little or no obstruction when moving between fiat and cryptoasset, or from cryptoasset-to-cryptoasset.").

[31] U.S. Dep't of the Treasury, *Financial Crimes Enforcement Network (FinCEN) Statement on Enforcement of the Bank Secrecy Act* (Aug. 18, 2020), https://www.fincen.gov/sites/default/files/shared/FinCEN%20Enforcement%20Statement_FINAL%20508.pdf.

[32] *See* U.S. Dep't of the Treasury, *Enforcement Actions*, https://www.fincen.gov/news-room/enforcement-actions.

treaty-based methods to get records from overseas); and consumers gain by being able to use VASPs subject to the broad array of domestic regulatory protections.

III. Treasury Should Continue to Collaborate with the Crypto Industry to Support Industry Compliance Solutions That Streamline Administrative Requirements, as Opposed to Mandating Specific Solutions[33]

To maintain the United States' technological leadership while protecting against emerging financial crime threats, it is vital that Treasury closely partner with the private sector, as acknowledged in the AMLA and consistent with this RFC. Industry stakeholders on the front lines of compliance are often the first to recognize emerging threats to the financial system and are well-placed to advise regulators on how to effectively respond while also mitigating other risks. Solutions developed in close collaboration with industry will generally more effectively mitigate risk than rules unilaterally issued, and we see real opportunities for impactful collaboration in two areas: decentralized identity tools and establishing a federal regulatory framework for payments regulation to cover both the transfer and storage of customers' crypto.

A. Treasury's Collaborative Approach to Travel Rule Compliance Offers an Effective Model that Should Be Replicated in Other Regulatory Areas

FinCEN has taken an effective approach to Travel Rule compliance by directly collaborating with industry to enable industry to solve a complex regulatory problem.[34] For traditional financial institutions, Travel Rule compliance is relatively straightforward: they can easily identify their financial institution counterparties and include Travel Rule data with the underlying transmittal orders. But for VASPs, the blockchain alone does not identify when a counterparty is another VASP, and there is no way to include Travel Rule data in the transmittal order itself. Thus, applying the Travel Rule to crypto transactions raises complex technical challenges around accurately identifying other VASPs and securely transmitting highly sensitive

[33] This section responds to the RFC's general request for input, as well as the following questions in the RFC: B1, B2, B4, D2, D4, D5, and D7.

[34] 31 C.F.R. § 1010.410(f) (requiring that U.S. financial institutions collect and retain records about fund transfers of $3,000 or more and pass on particular information—for example, their customer's name and address—to other financial institutions involved in the transfer).

Travel Rule data. When FinCEN announced that the Travel Rule would apply to crypto transactions,[35] it was unclear to the government and industry how to solve these challenges.[36]

But instead of passing new legislation or unilaterally dictating how to solve these complex challenges, FinCEN allowed and encouraged industry to find a solution and gave them the time to do so—and industry has successfully responded. Coinbase has worked alongside a large group of VASPs over the last few years to pioneer the development of a Travel Rule solution that allows members to accurately identify their counterparties and securely exchange required data, known as TRUST (the Travel Rule Universal Solution Technology). And we have invested significant legal, compliance, engineering, and other resources to build the TRUST platform, which VASPs are already using to exchange information required under the Travel Rule.

The TRUST solution's rapid growth since its launch earlier this year is a testament to the industry's commitment to solving complex compliance problems. For instance, all VASPs who join TRUST undergo comprehensive evaluations to help ensure that their security protocols are equipped to prevent unapproved access to sensitive customer data shared by TRUST participants. Further, TRUST was designed so that no PII is stored on a centralized database but is instead only shared directly between counterparty VASPs via encrypted, peer-to-peer channels, reducing the risk of hacking or improper access. These and other features have been critical to TRUST's growth to become the world's leading Travel Rule solution.[37]

Importantly, Coinbase engaged closely and repeatedly with FinCEN and other regulators while designing and launching TRUST. This approach of collaboration and encouraging industry innovation is far more effective than issuing unilateral rules that dictate how to solve certain concerns, without industry input on the actual risk, unintended consequences, and alternatives available. We encourage the Treasury to follow the approach it took with respect to the Travel

---

[35] FinCEN 2019 Guidance, at 11.

[36] *See* Kenneth A. Blanco, FinCEN Director, *Prepared Remarks of FinCEN Director Kenneth A. Blanco, Delivered at the Consensus Blockchain Conference* (May 13, 2020), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-consensus-blockchain ("We are encouraged that so many creative solutions are being developed by [the virtual currency] industry to address these Travel Rule obligations . . . . We have also previously highlighted our confidence that industry can absolutely carry out this requirement. We know technologies exist to support compliance with all recordkeeping obligations. Most challenges we see … relate to governance and process … many solutions in both governance and technology models could ultimately comply.").

[37] *See* Coinbase, *The Standard for Travel Rule Compliance: Travel Rule Universal Solution Technology*, https://www.coinbase.com/travelrule (describing the TRUST platform and listing VASPs who have joined the TRUST coalition).

Rule in seeking industry input to collaboratively understand other risks and develop effective solutions.

B. Treasury Should Encourage VASPs to Adopt Decentralized Identity Tools to Improve the Effectiveness and Efficiency of AML Compliance

One way in which Treasury could collaboratively work with financial institutions to increase adoption of new technology and analytics would be to encourage the use of decentralized identity (DID). Coinbase believes that DID will be a cornerstone of Compliance 3.0. However, several rules in the BSA currently limit VASPs' ability to effectively utilize DID. Treasury should amend these rules as suggested below and adjust regulatory expectations.

Traditional KYC mechanisms were developed in the context of opaque transactional ledgers and customer records, held by one firm and inaccessible to others. As a result, firms today largely rely only on their own identity verification processes, as opposed to capitalizing on verification work already done by other firms. This in turn requires customers to provide their personal information to *every* financial institution that they wish to establish an account with. By contrast, KYC based on DID holds the promise of being significantly more effective because it uses blockchain data that, as described above, is *immediate* (it is available on the blockchain as soon as the transaction happens), *independent* (it cannot be tampered with), and *dynamic* (it can be constantly reevaluated based on new information).

DID harnesses the unique advantages of the blockchain and sophisticated forms of encryption (for example, zero knowledge proofs)[38] to allow customers to confirm that they are who they claim to be, at times without even having to disclose their actual personal information. DID works by having a trusted entity, such as a financial institution, verify certain information about an individual (such as a birthdate, social security number, or the fact that they have undergone full KYC as of a certain date) and then issue them an attestation token confirming the fact at issue. The token holder, 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.[39]

---

[38] *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.").

[39] *See also* Financial Action Task Force, *Guidance on Digital Identity* ¶ 107 (Mar. 2020), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf ("FATF Digital Identity") (describing how digital ID systems can also provide more efficient experience for customers).

Similarly, a new financial institution opening an account for Jane could use her attestation token from a VASP that has already conducted full KYC on her. This streamlines the KYC process and frees up compliance resources for other effective compliance activities.[40] 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. VASPs can also incorporate all types of blockchain data into an attestation token, such as aggregate transactional information, to create a dynamic picture of the customer's risk profile.

Unfortunately, the regulatory landscape has not kept pace with this promising new technology, impeding efforts to capitalize on DID's potential. Under current law, financial institutions are required to take certain steps to know who their customers are and thus mitigate AML risks. For instance, banks are subject to what is known as the Customer Identification (CIP) rule,[41] while money services businesses (MSBs) must abide by general KYC requirements.[42] 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.[43] But neither the CIP rule nor FinCEN's guidance to date clarifies whether DID would qualify as a suitable "non-documentary method."

A similar ambiguity surrounds whether a VASP—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 may be able to offer DID services.[44]

---

[40] *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.").

[41] 31 C.F.R. § 1020.220.

[42] 31 C.F.R. § 1022.210(d)(1).

[43] 31 CFR § 1020.220(a)(2)(ii)(B).

[44] *See* 31 CFR § 1020.220(a)(6)(ii).

Coinbase commends FinCEN's recent efforts to promote the development of novel identity tools, such as the "Tech Sprint" it helped lead earlier this year.[45] And we would encourage even more on this topic. Until the underlying regulations are modified, or FinCEN issues 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.

C. Treasury Should Support the Creation of a Federal Framework for Payments Regulation, Replacing the Patchwork of State Regimes

Finally, Coinbase strongly supports Treasury's recommendation to establish a federal regulatory framework for payments regulation.[46] The need for a federal regulator in this space could not be greater given the increasing numbers of nonbank payment companies, including VASPs, whose operations extend far beyond state borders.

While Coinbase supports efforts by the Conference of State Bank Supervisors to reduce the regulatory burdens on nonbank payment providers,[47] a state-level regulatory structure does not account for the interstate and global nature of crypto. VASPs must maintain licenses in all states where required for them to offer their services, comply with all local laws, stay abreast of any legal and regulatory changes, and file necessary reports in the normal course of business to those state regulators.

A federal regulatory structure for nonbank payment providers would present an opportunity for Treasury to build a unified, national AML framework that could more adeptly counter emerging threats. It would further allow VASPs to utilize their compliance resources in a more effective manner.

---

[45] 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 efforts to understand how to use digital identity proofing to reduce money laundering and terrorist financing).

[46] *See* U.S. Dep't of the Treasury, *The Future of Money and Payments: Report Pursuant to Section 4(b) of Executive Order 14067*, at 47 (Sept. 2022) https://home.treasury.gov/system/files/136/Future-of-Money-and-Payments.pdf (recognizing that "[a] federal framework for payments regulation could support responsible innovation in payments").

[47] *See* Press Release, The Conference of State Bank Supervisors, State Regulators Roll Out One Company, One Exam for Nationwide Payments Firms (Sept. 15, 2020), https://www.csbs.org/regulators-announce-one-company-one-exam-for-payments-companies.

* * *

Coinbase appreciates the opportunity to work with Treasury to develop sound, effective regulation. By encouraging novel and collaborative approaches to combating illicit finance, Treasury can make regulatory and law enforcement efforts more effective while also ensuring that the United States remains at the forefront of innovation in financial services.

Sincerely,

DocuSigned by:
Paul Grewal
0E2CC8D881B5471...

Paul Grewal
Chief Legal Officer
Coinbase