**Circle Internet Financial, LLC**
99 High Street
Suite 1701
Boston, MA 02110

November 3, 2022

Deputy Assistant Secretary Scott Rembrandt
Office of Terrorist Financing and Financial Crimes
U.S. Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

Re: Federal Register Document 2022-20279

Dear Deputy Assistant Secretary Rembrandt,

Circle appreciates the opportunity to provide comments to the U.S. Department of the Treasury on digital assets-related illicit finance and national security risks, as well as on the action plan to mitigate risks as mandated by the White House *Executive Order on Ensuring Responsible Development of Digital Assets*. Since Circle's founding, we have prioritized responsible financial services innovation and constructive engagement with public authorities and regulators both in the United States and around the world.

## A. ILLICIT FINANCE RISKS

**1. Has the Treasury comprehensively defined the illicit financing risks associated with digital assets? Please list any key illicit financing risks that we have not raised in this Action Plan or the National Risk Assessment.**

The Treasury Department's efforts to comprehensively map and assess the risks that illicit actors pose to the safety and soundness of the digital assets market have resulted in valuable resources for the private sector. The risks identified in the February 2022 National Risk Assessment and the September 2022 Action Plan to Address Illicit Financing Risks of Digital Assets ("Action Plan") broadly align with Circle's view of the range of illicit finance threats and vulnerabilities, and establish a helpful foundation for anti-money laundering (AML)/combatting the financing of terrorism (CFT) risk management.

While the absolute value of illicit finance in digital assets has grown in recent years, Circle agrees with the Treasury Department's assessment that the use of virtual assets for money laundering remains far below that of fiat currency using more traditional methods. Industry studies further note that the growth of illicit finance in digital assets has not kept pace with overall user and market capitalization growth,[1] indicating a declining share of illicit activity relative to overall economic activity in the sector. This reflects Circle's understanding that the growth of the digital assets industry – and the rapid expansion in the area of decentralized finance (DeFi) – is not

[1] Chainalysis, January 2022, "Crypto Crime Trends for 2022" (https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/).

correlated with increased financial crime risk, and that high growth in these spaces does not proportionately benefit illicit actors.

Looking closer at the risks identified by Treasury, there is merit to further scoping them to balance competing financial policy objectives as well as to more effectively guide virtual asset service providers (VASPs) in tailoring their risk-based compliance regimes. The Action Plan identifies anonymity enhancing technologies as a key emerging illicit finance risk, focusing on complicit, unlicensed, and unregulated money services businesses (MSBs) that are likely deliberately avoiding compliance. While the Financial Action Task Force (FATF) recommends some anonymity-enhancing technology be treated as high-risk, it is our view that the technology is neither inherently nor categorically high-risk and can preserve an individual's privacy while mitigating AML/CFT risks (see response in section B6).

There are numerous licit use cases for why a user may wish to employ privacy technology in a public blockchain environment, just as there are numerous legitimate security reasons for an internet user to protect communications with encryption or a virtual private network (VPN). Such legitimate use cases may involve, for example, masking potentially exploitable personal identifying information, such as employment or salary details, or avoiding political scrutiny in making transactions, donations, or remittances to jurisdictions subject to heightened surveillance. The European Union – as part of its efforts to reconcile data privacy standards with the inherent openness of blockchain technology – has noted that public-key information alone can enable the identification of real-world identity and create a pattern of transaction activity that can be used to single out users,[2] underscoring the risks that the inherent traceability of blockchain can open users up to fraud, scams, and identity theft.

Like physical cash, anonymity enhancing technologies will continue to offer illicit actors a means of concealing the movement of funds; however, the general technology should be treated as a vulnerability that needs to be managed but not an inherent risk. We encourage the U.S. government to further scope the risks individual technologies pose to risk-management and due diligence guidance; to take advantage of potential improvements in compliance technology; and, to balance competing policy and legal requirements, such as those governing the disclosure of customer financial information.

**3. What are the illicit finance risks related to non-fungible tokens?**

The Bank Secrecy Act (BSA) does not yet encompass non-fungible tokens (NFTs); however, we recognize that the Treasury Department aims to complete a risk assessment of the sector by February 2023. While the category of NFTs is broad and can include anything from art and collectibles to representation of ownership over real-world goods (such as car titles and property deeds), the primary use case at this time is of the former. NFTs that are unique and non-interchangeable should not be considered virtual currency. Rather, such NFTs should be considered in relation to the underlying assets, for example, art or collectibles. We applaud the

[2] European Parliamentary Research Service, July 2019, "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?" (https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf).

Treasury's acknowledgement of NFTs in its study[3] on the risks posed by trade in works of art. Furthermore, we recommend that NFT dealers, that are not otherwise considered VASPs, be subject to the same AML requirements as dealers in works of art. We recognize that money laundering and terrorist financing risks increase with the value of the NFT; therefore, the thresholds proposed by the Treasury Department in its recent study appear reasonable.

At this time, Circle does not see the need to amend the BSA to make explicit that its key AML/CFT provisions apply to NFT platforms, as put forward by the U.S. Department of Justice's recent proposal,[4] without the U.S. government first clarifying which NFT platforms fall under the VASP definition.

In examining the potential use to terrorist groups, it is important to differentiate between NFTs' use as money laundering mechanisms and the importance of the underlying tokenized object, which can carry separate value to terrorist groups as communications or propaganda that may be difficult for authorities to address. For instance, in September 2022, former senior U.S. intelligence officials publicly acknowledged the first NFTs created and disseminated by a terrorist sympathizer.[5] NFTs are more difficult to censor than, for example, a news release on a conventional website; thus, even if major NFT platforms, such as OpenSea and Rarible, remove them, NFTs still survive on a blockchain. Therefore, in addition to potentially funding terrorism or terrorist groups, NFTs could be used to spread information, which could lead to larger membership for terrorist organizations and indirect growth of their coffers.

**4. What are the illicit finance risks related to decentralized finance (DeFi) and peer-to-peer payment technologies?**

DeFi has grown significantly since 2020 and become a prominent feature of the evolving digital assets ecosystem. This growth has naturally led to increased attention regarding the potential AML/CFT compliance challenges that stem from applying existing AML/CFT compliance guidance to this space. The widely-recognized core AML/CFT vulnerability remains the permissionless nature of these services, allowing individual users to conduct transactions without intermediaries to handle standard AML processes. This creates two broad risk categories: 1) money laundering risk from illicit actors seeking to generate or launder the proceeds of crime pseudo-anonymously and 2) a heightened risk of fraud, hacks, and other cyber crime to DeFi users. Overall, the declining share of illicit activity as a percentage of digital asset growth since 2020[6] – a period characterized by large growth in DeFi – and surge in DeFi cyber theft reflects that the latter poses the more material risk of illicit finance in DeFi. While financial crime writ large in DeFi grew by more than 2,000% between 2020 and 2021, the growth was disproportionately driven by scams and theft of cryptocurrency within the DeFi space itself rather than money laundering,

---

[3] U.S. Department of the Treasury, February 2022, "Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art" (https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf).
[4] U.S. Department of Justice, September 2022, "The Role Of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets" (https://www.justice.gov/ag/page/file/1535236/download).
[5] Wall Street Journal, Ian Talley, September 2022, " Islamic State Turns to NFTs to Spread Terror Message" (https://www.wsj.com/articles/islamic-state-turns-to-nfts-to-spread-terror-message-11662292800).
[6] Chainalysis, January 2022, "Crypto Crime Trends for 2022" (https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/).

according to blockchain analytic research.[7] In the first half of October 2022 alone, hackers stole more than $700 million from DeFi markets, pushing the 2022 total above $3 billion and well ahead of the pace of previous years.[8]

A recent review of users' holdings of stablecoins and tokenized cash found that the majority of accounts, including individual wallets and institutional custody wallets, were made up of low-value, externally-owned accounts.[9] While not a direct measure of DeFi usage, externally-owned stablecoin accounts could indicate decentralized or peer-to-peer accounts because of the wide use of stablecoins as an on/off-ramp and store of value in the DeFi space. Notably, around 75% of the 2 million individual wallets on the Ethereum blockchain holding USDC had balances of less than $100. In total, 95% of all USDC wallet holders held less than $10,000.[10] This high ratio of low-value individual wallets reflects the composition of the DeFi sector as largely individual digital asset users and traders and suggests that the aggregate money laundering risk – particularly arising from bulk money laundering – within the decentralized digital asset ecosystem remains low despite a large number of users. The relative scarcity of wallets holding more than $10,000 also suggests that the ability to obscure or wash the proceeds of crime diminishes in relation to the transaction size.

While illicit actors likely use, and will continue to use, individual wallets and DeFi for laundering the proceeds of crime, it is our understanding that DeFi users remain comparatively more vulnerable to being the victims of illicit activity. In turn, illicit actors within the DeFi ecosystem are likely to be most vulnerable at the points of entry and exit. DeFi relies primarily on centralized on/off ramps such as exchanges, borrowing/lending platforms, and other VASPs for the conversion to/from fiat. These on/off ramps have a more clearly defined compliance burden and present the greatest exposure of illicit actors to customer due diligence measures, increasing the difficulty for illicit actors to convert funds to fiat, particularly at scale.

**B. AML/CFT Regulation and Supervision**

**1. What additional steps should the United States government take to more effectively deter, detect, and disrupt the misuse of digital assets and digital asset service providers by criminals?**

The U.S. government plays a leading role in setting the global standards that act as a deterrent against abuse of the digital assets space and that aid domestic and international entities in identifying, regulating, and supervising emerging trends in illicit finance. The inherent characteristics of blockchain technology give it the potential to more effectively and efficiently fight money laundering, terrorist financing, and other forms of illicit finance; and, as noted in the comprehensive framework for addressing digital assets, the United States stands to lose ground

[7] Chainalysis, January 2022, "Crypto Crime Trends for 2022" (https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/).
[8] Coindesk, October 13, 2022, "October Becomes Worst Month for Crypto Hacks With Two Weeks to Go" (https://www.coindesk.com/tech/2022/10/13/october-becomes-worst-month-for-crypto-hacks-with-two-weeks-to-go/).
[9] Gordon Liao, 23 September 2022, "Macroprudential Considerations for Tokenized Cash," (https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4228268_code2769759.pdf?abstractid=4228268&mirid=1).
[10] Ibid.

in promoting the rule of law if it does not modernize its approach to blockchain technology. Circle appreciates the financial advisories that Treasury publishes on a periodic basis which seek to alert financial institutions to emerging risks and associated red flags and typologies in order to better protect the U.S. financial system. Like all mediums of exchange in the financial system, however, criminal actors continually evolve their use of financial tools to support their illicit activities. As a result, it is ever more important that Treasury advisories accurately reflect the differences between traditional and digital assets, looking not just at the risks and vulnerabilities but also at the emerging tools that can be used to spot and mitigate illicit behavior. More nuanced typologies and red flags would also improve the relevancy and usefulness of Suspicious Activity Report (SAR) filings which, in turn, will enhance future advisories and public-private engagement. We also recognize the Financial Crime Enforcement Network's (FinCEN) efforts to revise, update, and revoke advisories when appropriate. Circle would encourage a more regular review of the typologies and red flags related to digital assets in existing advisories, since the risks associated with digital assets products change with advancements in the technology. Advisories that have not been rescinded should be maintained to have accurate typologies and red flags.

FinCEN's publication of government-wide priorities for AML/CFT policy ("the Priorities") was a timely and informative update on the most pressing threats to the U.S. financial system. Though the issuance of these Priorities was mandated by the Anti-Money Laundering Act of 2020 (AMLA) and FinCEN publicly stated that it will update the Priorities at least once every four years as required by the AMLA, Circle believes that covered entities would be best served by a more frequent update to or reaffirmation of national AML/CFT Priorities. As FinCEN noted recently, "we have to ensure our AML/CFT regime reflects modern national security needs,"[11] and the private sector can only do so if they have clear direction from the Treasury Department about national security priorities.

Additionally, Treasury noted in its "Future of Money" report the importance of developing identity verification sufficient to enable AML compliance while balancing user privacy.[12] Supporting the development of digital identity tools and international standards around digital identity management would aid both the private sector and U.S. government in the detection and reporting of illicit financial activity. Industry-driven tools such as Verite[13] and the Travel Rule Universal Solution Technology (TRUST)[14] are creating platforms that allow streamlined identity certification and the transmission of information required by the Travel Rule. Engagement with industry to support adoption of novel means of digital identity or Know Your Customer (KYC) as well as on more surgical approaches to targeting illicit actors' use of designated services would aid in disruptive efforts while minimizing collateral impact on licit users.

---

[11] Him Das, January 2022, "Prepared Remarks, Him Das, Acting Director, Financial Crimes Enforcement Network, American Bankers Association/American Bar Association Financial Crimes Enforcement Conference" (https://www.fincen.gov/news/speeches/prepared-remarks-fincen-acting-director-him-das-delivered-virtually-american-bankers).

[12] U.S. Department of the Treasury, September 2022, "Future of Money and Payments" (https://home.treasury.gov/system/files/136/Future-of-Money-and-Payments.pdf).

[13] Verite is an open-source framework for proving identity claims without exposing sensitive personal information. For more on Verite, see https://www.circle.com/en/verite.

[14] TRUST is an industry-created compliance tool to allow VASPs to securely communicate certain basic customer information when sending funds in compliance with the FATF's "travel rule." For more on TRUST, see https://www.circle.com/blog/introducing-the-travel-rule-universal-solution-technology.

Equally important to issuing clear and comprehensive guidance is ensuring that similar services with similar risk profiles are regulated in a similar fashion. The global fungibility of digital assets, combined with differing AML/CFT standards, allows illicit USD-denominated activity outside of the U.S. regulatory perimeter. We encourage the Treasury Department to clarify customer due diligence, suspicious activity reporting, and sanctions obligations for foreign VASPs that serve U.S. customers and provide USD-denominated services, which would aid in the detection of illicit activity and serve as a stronger deterrent against AML/CFT regulatory arbitrage.

**2. Are there specific areas related to AML/CFT and sanctions obligations with respect to digital assets that require additional clarity?**

Given the centrality of KYC controls to both AML/CFT and sanctions obligations, digital identity tools can provide a verifiable and proven identification mechanism that is scalable, usable by anyone, and interoperable across digital asset systems (for further detail see response B6). The Treasury Department should develop guidance and standards for KYC services based on digital identity technology. Both third-party and open-source digital identity solutions are in use today that enable KYC "on-chain" and address or reduce some of the key risks and vulnerabilities identified in the National Risk Assessment and Action Plan, notably regarding cross-border regulatory gaps, disintermediation, and non-compliance. Establishing digital identity guidance for individual wallet owners; credentialing; privacy preserving tools using technology such as zero-knowledge proofs (ZKP);[15] and, the use of third-party digital KYC tools would support implementation of robust KYC controls across the digital asset space and promote standardization centered on U.S. regulations. Such guidance would have the added benefit of incentivizing covered entities to invest in and develop robust customer due diligence and develop cross-protocol, open-source digital identity solutions.

With respect to sanctions, Circle appreciates the guidance and clarifications issued by the Office of Foreign Assets Control (OFAC) which have explained some of the obligations resulting from recent actions. However, further guidance with respect to mixers and anonymity-enhancing services would aid VASPs in developing risk-based compliance regimes and avoiding de-risking of customers, services, or protocols because of overcompliance or based on risks that could be effectively managed with existing digital identity tools (for further detail see response B5).

**3. What regulatory changes would help better mitigate illicit financing risks associated with digital assets?**

As the Treasury Department's Action Plan notes, uneven and inconsistent regulation of digital assets allows illicit actors to engage in regulatory arbitrage due to the near-instantaneous and borderless nature of digital asset transfers. Currently, U.S. persons can use similar USD-pegged tokens and services that are subject to different jurisdictions' requirements for customer due diligence, KYC, sanctions compliance, and data collection and retention. Moreover, some token issuers and service providers seek out jurisdictions that have limited or no demonstrable AML/CFT requirements for VASPs. This would potentially allow VASPs to offer services to U.S. consumers and/or reference the U.S. dollar without sufficient compliance programs, exposing U.S. persons to AML/CFT risk. Regulatory discrepancies and VASPs playing regulatory arbitrage

[15] Zero-knowledge proofs are a cryptographic method for proving to a third-party that a given statement is true while avoiding conveying the underlying information apart from its validity.

could lead to consolidation of illicit funds movement, potentially involving a USD-pegged token, outside of the U.S. regulatory perimeter.

The Treasury Department guidance notes that certain activities by non-U.S. persons that involve the United States, U.S. persons, or goods or services exported from the United States may be subject to Treasury sanctions regulations. OFAC further notes that "anyone engaging in virtual currency activities in the United States, or that involve U.S. individuals or entities, should be aware of OFAC sanctions requirements and the circumstances in which they must comply with those requirements… Additionally, in most sanctions programs, any transaction that causes a violation — including a transaction by a non-U.S. person that causes a U.S. person to violate sanctions — is also prohibited."[16] However, the regulations applying these requirements for U.S.-registered MSBs without a U.S. presence and for non-U.S. entities serving U.S. persons could be clarified to prevent different interpretations of U.S. sanctions; differing interpretations have resulted in inconsistent application of freezing measures, which could incentivize illicit actors to seek non-U.S. VASPs offering services to U.S.-based entities.

From the consumer perspective, U.S. persons can readily avail themselves of tokens potentially without knowledge of the additional money laundering or terrorist financing risk to which they may be exposed. Recognizing the difficult and different challenges of aligning cross-jurisdiction regulation, we encourage the Treasury, in the meantime, to clarify regulations on service provision to U.S. persons, which would help users and VASPs appropriately assess risks, enforce sanctions obligations, and file SARs.

The compliance obligations of covered entities for the third-party use of digital asset offerings is another area that merits further regulatory clarification given the novel facets of the sector. Existing guidance does not mandate that financial institutions dealing in digital assets conduct monitoring using blockchain analytics nor does it specify the extent to which monitoring must be conducted as a compliance measure or whether, and to what extent, such measures should be applied to customers' customers. However, recent Treasury guidance noting that sanctions regulations apply to unsolicited virtual currency transactions with designated persons[17] raises questions about the extent to which the compliance burden for VASPs and individual users apply to downstream customers using funds linked to sanctioned persons.

Furthermore, this existing guidance (that VASPs' customers who have received unsolicited funds — i.e. that have no apparent *voluntary* link to designated persons — have reporting and blocking obligations) becomes more opaque with respect to assets that were kept in circulation — for example, due to use by foreign persons not subject to U.S. sanctions regulations — that by virtue of the fungibility and traceability of blockchain technology can connect downstream unaffiliated U.S. persons to SDN activity. Furthermore, digital assets that have or may be unblocked due to an approved OFAC specific license may be treated with undue suspicion once sent from the original wallet.

[16] OFAC, October 2021, "Sanctions Compliance Guidance for the Virtual Currency Industry" (https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf)
[17] OFAC, 13 September 2022, "FAQ 1078. Do OFAC reporting obligations apply to 'dusting' transactions?" (https://home.treasury.gov/policy-issues/financial-sanctions/faqs/1078).

**4. What additional steps should the U.S. government consider to combat ransomware?**

Circle believes that there have been (and will continue to be) many legitimate use cases for financial privacy that can be harmonized with the ability for law enforcement to trace and prosecute illicit financial activity.

In the course of observing ransomware-driven illicit financial activity, major blockchain analytics firms have noted that criminals are moving away from mixing services and toward the use of privacy coins (also known as anonymity-enhancing coins, or AECs) due to the proliferation of tracing tools and activity by entities such as OFAC. The Treasury Action Plan concurs, stating that "FinCEN indicates that some ransomware actors have demanded payment in anonymity-enhanced cryptocurrencies (AECs), requiring an additional fee for payment in bitcoin or only accepting payment in bitcoin after negotiation." While bitcoin remains the predominant vehicle for ransomware payments today, these findings highlight the increased use of privacy enhancing tokens and services by bad actors to obfuscate the sender, receiver, and amount to launder the proceeds of ransomware.

While illicit actors engaging in ransomware attacks clearly favor certain digital assets and continue to use bridges to launder proceeds, the rise of these attacks cannot be divorced from the underlying cybersecurity vulnerabilities unrelated to digital asset infrastructure. In fact, compromised remote desktop protocol connections made up the largest attack surface for ransomware in 2021, with VPNs comprising the most commonly exploited software vulnerability.[18] In the absence of such weaknesses, ransomware programs would not be able to penetrate valuable networks, and bad actors would have a harder time reaching data that could be encrypted for sale. Without addressing these vulnerabilities, tracking ransomware flows through AECs and bridges will remain a perpetual game of cat and mouse that fails to address the underlying issue.

*Anonymity-Enhancing Coins (AECs)*

Privacy coins, or AECs, allow for greater transaction anonymity than asset transfers conducted using bitcoin or the Ethereum network, but can be hard to source from exchanges in the United States due to regulatory uncertainty and small market capitalization (a total of $5.2 billion for all AECs compared to approximately $150 billion in stablecoins).[19] The two most popular AECs by market capitalization are Monero ($2.5 billion) and Zcash ($790 million),[20] which work through cryptographic methods to obscure transaction details that would normally allow for the tracing of financial flows on the blockchain. For example, transactions using Monero operate through a system ring signatures, which allow signing on behalf of a group of wallet addresses to conceal the sender and receiver of a transaction.[21] Zcash harnesses ZKPs to confirm verifiably that a

[18] Panda Security, 05 March 2022, "73 Ransomware Statistics Vital for Security in 2022" (https://www.pandasecurity.com/en/mediacenter/security/ransomware-statistics/).
[19] Coinmarketcap, 21 October 2022, "Top Privacy Tokens by Market Capitalization" (https://coinmarketcap.com/view/privacy/)
[20] Ibid.
[21] Cronokirby, 07 March, 2022; "On Monero's Ring Signatures" (https://cronokirby.com/posts/2022/03/on-moneros-ring-signatures/).

transaction has occurred while keeping crucial details encrypted (unless legally or voluntarily revealed by either counterparty) to outside observers.[22]

Despite potential AML/CFT vulnerabilities inherent in the capabilities of all privacy coins, it should be noted that research suggests that these two AECs diverge fundamentally in their use by criminal actors. A 2020 study by the Rand Corporation found that there continues to be no widespread use of Zcash for criminal activity, though the report recommends vigilance to prevent such activity from emerging.[23] To ensure greater compliance with AML/KYC measures, the U.S. government should work to clarify standards for VASPs that list privacy coins and promote digital identity standards for protocols that integrate with privacy coins or networks. Because bitcoin is still perceived to be the most dominant cryptocurrency for the completion of ransomware payments and illicit finance, we encourage a continued risk-based focus of law enforcement efforts on such transactions, even as the perimeter is extended to catch illicit actors turning to AECs.[24]

*Cross-Chain Bridging*

As with privacy coins, cyber criminals have repeatedly been observed using bridges to transfer funds away from the "scene of the crime," as cross-chain bridges allow attackers to obfuscate the flow of ransom payments by moving between multiple smart contracts in the bridging process, or additionally, to store funds on blockchains that are less resilient to blocking or seizure.[25] Unlike AECs, however, bridges represent a critical piece of blockchain infrastructure that enable both digital asset interoperability and adoption, and must not be limited unnecessarily. Decentralized exchanges are a potential opportunity; however, Elliptic found that due to liquidity constraints, attackers frequently need to swap tokens within a target blockchain to be able to move funds across these bridges, and that this utilization of decentralized exchanges may serve as a bottleneck for illicit activity as well as a chance to intercept attackers.[26]

Cross-chain bridges come in several architectures which complicate tracking and recovery efforts, but fundamentally serve the same purpose for ransomers. These bridges may consist of two smart contracts which custody assets on either side, or as a messaging protocol between two platforms (such as the Cosmos Inter-Blockchain Communication Protocol) which do not custody assets from swaps directly. A bridge may also issue a "wrapped" version of a token on a corresponding chain, which is a representation of a native asset (such as bitcoin) on a smart contract compatible blockchain. Bridges of both varieties can help ransomers evade blockchain analytics firms and also prevent the recovery of ransomed funds, and thus should be the source of increased engagement with the private sector by the Treasury Department. Bridges also hae positive benefits for the digital assets ecosystem, aiding users in legitimate transfers of digital assets across blockchains, ultimately enhancing the use cases of certain tokens.

---

[22] Electric Coin Company, 2021, "How It Works" (https://z.cash/technology/).
[23] Erik Silfversten, Marina Favaro, Linda Slapakova, Sascha Ishikawa, James Liu, Adrian Salas, 2020, "Exploring the use of Zcash cryptocurrency for illicit or criminal purposes" (https://www.rand.org/pubs/research_reports/RR4418.html).
[24] Ibid.
[25] Eray Arda Akartuna, Thibauld Madelin, 2022, "The State of Cross-chain Crime" (https://www.elliptic.co/hubfs/State%20of%20cross-chain%20crime/Elliptic_Cross-Chain_Crime_Report.pdf)
[26] Ibid.

**5. What additional steps should the U.S. government consider to address the illicit finance risks related to mixers and other anonymity-enhancing technologies?**

The intersection of privacy, open software, and security has warranted consolidated policy action, education, and advocacy. Treatment of individual financial privacy within the current traditional finance system and the BSA's regulatory framework is rapidly becoming outdated as cryptography, open software, and universally accessible personal wallets create opportunities for a more inclusive economy as well as risks to personal data. Fundamentally, privacy is not at odds with financial crimes compliance, but tools and software that are co-opted by bad actors cannot go unchecked. Public blockchains, blockchain forensics, and financial analytics have enabled broader investigations into illicit financial flows.

Recent Treasury action on a privacy mixer raised new compliance challenges that do not exist in traditional finance. For example, after the designation of Tornado Cash, small amounts of ETH were sent unsolicitedly from the Tornado Cash Designated Smart Contracts to public wallets, including those held by U.S. persons. Given the nature of digital assets, these individuals could not refuse the ETH; the only existing analogy to dusting would be a criminal depositing stolen cash in an individual's bank account with a note proving that the cash was illicit. Those individuals, due to the pseudo-anonymity of public wallet addresses, now have illicit funds in their wallets and are subject to the burden of blocking reporting obligations to the Treasury Department.

Furthermore, many U.S. persons who used Tornado Cash prior to August 8, 2022 and interacted with the now-designated liquidity pool smart contracts, or were the recipient of dusting attacks following designation, may have had their funds and/or wallets blocked due to the sanctions compliance controls of receiving parties. Many exchanges, wallet service providers, payment services providers, and other institutions have put in place sanctions compliance programs that will reject/block transactions with addresses that pose direct as well as indirect (1 to 2 hops) exposure to OFAC-sanctioned addresses. The Tornado Cash designation can "taint" and thereby render inoperable many hosted and self-hosted wallets that were exposed, either purposefully or inadvertently, to designated Tornado Cash addresses before and after August 8. This creates an undue challenge for users who can no longer access or move their digital assets due to tainting.

The guidance that OFAC issued stating that individuals who have been dusted could apply for a specific license was a positive step in clarifying OFAC's policy positions and the industry's obligations for sanctions compliance, even if a general license would have further mitigated unintended consequences to U.S. persons engaged in licit activities. However, OFAC did not provide any guidance to individuals or compliance professionals about how to ensure that dusted funds and wallets are not further tainted once a specific license is granted. While funds may be unblocked by an exchange or individual as a result of a specific license, the wallet's nexus to Tornado Cash will be visible on-chain while the specific license is not. Such users may have secondary compliance ramifications as a result.

Finally, from our conversations within the industry, there is a clear demand for dialogue with OFAC to identify more surgical approaches that would render illicit actors unable to use designated services while mitigating impact of similar designations on licit users. Unless the majority or entirety of users with funds in those pools have ties to illicit activity, Circle urges OFAC to consider avoiding the designation of liquidity pool smart contracts in favor of application node

addresses that enable the functioning of decentralized applications and services. Several of the 44 addresses listed by OFAC for Tornado Cash serve functional roles for the Tornado Cash application, i.e., routers, relayers, and mixers. If the primary purpose of designating Tornado Cash or any similar targets (decentralized applications and networks pooling many users' funds) is to prevent illicit actors – including the likes of the Lazarus Group and other sophisticated cyber actors – from using these tools, freezing liquidity pools could have more significant secondary impacts than what was intended.

**6. What steps should the U.S. government take to effectively mitigate the illicit finance risks related to DeFi?**

Without a regulatory framework, criminal or sanctioned entities may employ DeFi protocols to launder money or evade sanctions with little fear of repercussion given the disproportionate use of DeFi for hacks, scams, and cybercrime (as noted previously). While a recent report by Chainalysis found that illicit finance continues to make up only .05% of all blockchain-based transactions to-date, DeFi developers can and should take steps to build in effective controls to prevent this activity with additional guidance and regulation.[27] Additionally, developing and publishing standards around KYC and digital identity would give builders a path to embed protections directly into their protocols from the beginning, rather than only in response to discovery of widespread vulnerabilities. In addition to clear regulation, law enforcement entities might benefit from further education on how to trace and scope illicit finance investigations in the DeFi space, more effectively harnessing the transparent nature of distributed ledgers and emerging technologies while avoiding de-risking of services or protocols.

*Digital Identity Solutions*

Consumers would benefit from administrative rulemaking that establishes requirements for KYC controls based on digital technology. Both third-party and open-source identity solutions have been developed to enable KYC "on-chain," even as a universal standard has yet to be implemented. Ideally, a digital identity model would provide a verifiable and proven identification that is scalable, usable by anyone, and interoperable across systems, while also providing individuals the certainty that only the minimal amount of information will be shared.[28] Such systems are possible via cryptographic proofs and promise to overcome the current inefficiencies and risks associated with data silos maintained by financial institutions.

In an effort to further develop these solutions, Circle and other leading VASPs in the United States have partnered together to publish a set of free, open-source digital identity protocols and data models, called Verite. These protocols allow users and institutions to cryptographically prove claims about their identities and to allow services to attest to those claims while avoiding exposure of a user's sensitive data. Should these credentials reach widespread adoption, illicit actors would face increased friction when trying to operate without a verified identity, though international standards would need to be well-enforced so as to prevent illicit actors from moving

[27] Mengqi Sun, 26 January 2022, "DeFi Increasingly Popular Tool for Laundering Money, Study Finds" (https://www.wsj.com/articles/defi-increasingly-popular-tool-for-laundering-money-study-finds-).
[28] Example: Forbes, 2017, "The Equifax Breach and the Case for Digital Identity" (https://www.forbes.com/sites/dantedisparte/2017/10/02/the-equifax-breach-and-the-case-for-digital-identity/?sh=160605634e24).

to more lax jurisdictions. Harnessing several well-tested identity frameworks, Verite allows a credentialed issuer to create a "cryptographic badge" upon successful completion of KYC for each customer, which can then be presented at the user's direction whenever authentication is needed on the network. This architecture would mean that fewer actors would hold personal identifying information that might be leaked or exploited online, as only a cryptographic verification function would be necessary for attestation which would sit in the user's digital wallet.

Such a solution ensures that only minimal data is stored transparently on-chain, with the full identity available to law enforcement through a subpoena of the credential issuer similar to existing BSA systems. While other, more decentralized protocols have been proposed in the form of non-transferable NFTs, Circle believes that the Verite standard achieves the greatest balance of privacy and compliance. Regardless of government standard for digital identity technology, issuers that hold customers' KYC information would need to store it pursuant to the highest security standards in order to prevent leakage or theft and subject to existing BSA financial information sharing limitations.

*Permissioned Pools and Other Technologies*

Permissioned DeFi pool standards for users with digital identity credentials could provide another way to mitigate potential illicit activity. Such a pool could, for example, verify a user's credentials before allowing them to deposit funds; using this model, pool operators could likely prevent access to a pool by illicit actors and avert the intermingling of stolen assets with legitimate ones by requiring a verified digital identity credential. Of course, the benefits of limiting illicit activity through such a feature should be sought without eliminating the wider utility of permissionless DeFi to revolutionize financial access and frictionless lending and borrowing, and must be considered in this context. It is possible to have robust AML/CFT controls while balancing other policy objectives as well, such as the desire to ensure that financial services are accessible to disadvantaged and vulnerable populations. Circle is committed to extending financial services to historically underserved populations while maintaining a high standard of AML/KYC compliance.

Practically, strong public outreach and engagement will be critical to promoting risk management within the DeFi market. We encourage the Treasury Department, in cooperation with other federal banking agencies, to actively promote cross-industry collaboration and solutions that are risk-based and technology-neutral. Regulators should give institutions safe harbors, innovative sandboxes, and more regulatory clarity in order to adopt digital identity systems into existing AML/CFT programs. Furthermore, FinCEN should allow covered entities to rely on certified digital identity providers to comply with BSA regulations, as a similar precedent has already been set by Customer Identification Program reliance provisions.[29]

## C. GLOBAL IMPLEMENTATION OF AML/CFT STANDARDS

**1. How can Treasury most effectively support consistent implementation of global AML/CFT standards across jurisdictions for digital assets, including virtual assets and virtual asset service providers?**

The United States has the potential to play a leadership role in setting international standards for

[29] Examples: 31 CFR 1020.220 (a)(6) for banks and 31 CFR 1023.220 (a)(6) for broker-dealers.

AML/CFT regulations around digital assets at a pivotal time in the development of a host of state-sponsored and private digital assets systems. Many countries are currently considering a variety of regulatory frameworks, but materially-different requirements from one country to another significantly increase the cost of compliance to a nascent industry and open the door to a "race to the bottom" among countries that offer lax regulatory regimes. The United States can serve as a standard bearer bilaterally and through standard-setting bodies like FATF to harmonize rules that meet U.S. standards. The Treasury Department should continue to act as the coordinating body among other departments and agencies in the U.S. government to establish regulatory clarity internationally so that the benefits of digital assets are not hindered by their current AML/CFT risks.

**2. Are there specific countries or jurisdictions where the U.S. government should focus its efforts, through bilateral outreach and technical assistance, to strengthen foreign AML/CFT regimes related to virtual asset service providers?**

Circle appreciates the work done by the Treasury Department at the FATF to establish international standards and best practices for AML/CFT compliance in the digital assets space. The U.S. government's efforts to create regulatory harmony benefit consumers, businesses, and the safety and soundness of the global financial sector. Circle encourages the U.S. government to continue playing an active role in standard setting through a comprehensive domestic regulatory framework for digital assets, promoting global implementation of FATF standards, and conducting targeted engagement to address discrepancies in AML/CFT regulation.

Specifically, we encourage close coordination with European Union authorities on the implementation and reconciliation of EU data protection standards with existing AML/CFT requirements, given the impacts that data minimization, the right to erasure, protection of personal data, and other privacy questions may have on cross-border customer due diligence and U.S. VASP compliance. With the EU Data Protection Board currently developing guidelines for blockchain technology, transatlantic alignment on AML/CFT and privacy guidance as well as cooperation on the framework for privacy-preserving compliance tools takes on added urgency.

With regard to technical assistance, we encourage the Treasury Department to take a demand-focused approach and prioritize jurisdictions where there are large volumes of individual transfers – such as remittances – from the United States or growing local reliance on mobile or digital payments services. The World Bank estimates that global remittance flows will top $630 billion in 2022 and identified the top five recipients of remittances as a share of GDP in 2021 as Lebanon (54%), Tonga (44%), Tajikistan (34%), Kyrgyz Republic (33%), and Samoa (32%).[30] Circle has seen significant growth in adoption of USDC in such jurisdictions; for example, in Mexico, there has been a 400% increase in remittance volume using USDC which now makes up about 5% of annual U.S.-Mexico remittance volume. Focusing on the materiality of the cross-border payment and remittance industry would suggest that emphasis should be placed on the Middle East, Africa, and Latin America where remittances saw upwards of 20% growth in 2021.[31]

[30] World Bank, May 2022, "Remittances to Reach $630 billion in 2022 with Record Flows into Ukraine,: (https://www.worldbank.org/en/news/press-release/2022/05/11/remittances-to-reach-630-billion-in-2022-with-record-flows-into-ukraine#:~:text)

[31] World Bank, November 2021, "Remittance Flows Register Robust 7.3 Percent Growth in 2021," (https://www.worldbank.org/en/news/press-release/2021/11/17/remittance-flows-register-robust-7-3-percent-growth-in-2021)

**D. Private Sector Engagement and AML/CFT Solutions**

**1. How can Treasury maximize public-private and private-private information sharing on illicit finance and digital assets?**

While 31 U.S.C. 5312(a)(2) – the definition of "financial institutions" – explicitly names different types of MSBs as covered entities and, therefore, included in outgoing requests pursuant to 314(a) of the USA PATRIOT Act, in practice, 314(a) requests are not sent to many MSBs. Because MSBs may have data that is responsive to an investigation, it is not uncommon for law enforcement to send MSBs, particularly VASPs, "fishing" subpoenas that request information for an individual, email address, or cryptocurrency address. The 314(a) process is less burdensome than other methods like subpoenas and provides FinCEN and law enforcement more timely data. Circle would prefer outreach using the 314(a) process.

Section 314(b) of the USA PATRIOT Act is an important mechanism for financial institutions to share information under a safe harbor provision, and we commend FinCEN's efforts recently to widen the types of entities that can participate. While participation is voluntary, we appreciate FinCEN and, more broadly, the Treasury's efforts to encourage financial institutions to be active members in order to aid efforts to fight money laundering, terrorist financing and financial crime. To this point, because the inherent characteristics of blockchain technology give it the potential to more effectively and efficiently fight money laundering, terrorist financing, and other forms of illicit finance, partnerships between VASPs and financial institutions would maximize visibility into on/off ramps to fiat currency.

Finally, in accordance with Priority Action 6 set out in Treasury's Action Plan,[32] Circle believes that establishing a forum for policymakers, regulators, and financial institutions to engage and learn more about the blockchain-based tools and products can improve industry compliance.

**2. How can the U.S. Department of the Treasury, in concert with other government agencies, improve guidance and public-private communication on AML/CFT and sanctions obligations with regard to digital assets?**

Proactive guidance from the Treasury Department at the time of designation can mitigate many of the unintended consequences of sanctions and instead truly target illicit entities. General licenses and wind down periods provide legitimate actors the ability to modify behavior to comply with sanctions. Broadly speaking, however, sanctions are an ineffective way to communicate Treasury policy to the private sector. While sanctions have been shown to disrupt illicit actors, most frequently, such actors reconstitute their operations through other permissive environments. This makes the implementation of AML/CFT standards worldwide even more important, as illicit actors will look for permissive jurisdictions to continue their activity.

Given the unique aspects of countering illicit financial flows on blockchains and with digital assets, Treasury could consider pre-designation consultations with select members of the digital assets community in order to anticipate the potentially novel consequences that might arise from

[32] U.S. Department of the Treasury, September 2022, "Action Plan To Address Illicit Financing Risks of Digital Assets" (https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf)

intended sanctions. While there is a justified concern about asset flight and therefore designations are always classified and/or not shared with the public, there could be an opportunity to have protected conversations with members of the private sector who, for instance, might still retain security clearances. This could also allow OFAC to have additional insight into sanctions and AML violations.

3. **How can Treasury encourage the use of collaborative analytics to address illicit financing risks associated with digital assets while also respecting due process and privacy?**

The work of blockchain analytics firms has been central to tracking and reporting the flow of illicit finance in the digital asset ecosystem, as well as to pushing back on misconceptions that digital assets increase the ability for bad actors to engage in money laundering. Existing guidance does not mandate that covered entities dealing in cryptocurrency conduct monitoring using blockchain analytics, nor does it specify the extent to which monitoring must be conducted. FinCEN could consider enhancing guidance to require that financial institutions conducting blockchain transactions must monitor said transactions using blockchain analytics technology to identify suspicious transactions, and what it defines as suspicious transactions. For example, whether a transaction directly to a darknet marketplace is, in and of itself, suspicious, or is such a transaction only suspicious in connection with other risk indicators.

Financial institutions may also benefit from additional guidance regarding the number of hops or speed at which funds move when determining whether activity is considered to be suspicious. As a result, the Treasury Department should encourage guidance that requires those financial institutions conducting distributed ledger transactions to use blockchain analytics technology that identifies suspicious financial flows. Furthermore, given the increased transparency inherent in blockchain technology, FinCEN should consider providing guidance on how far BSA obligations extend for covered institutions.

*Privacy Tools*

Market demand has encouraged the development of new technologies that safeguard a user's privacy while still remaining compliant with AML/CFT obligations, and the Treasury Department should seek to tap into these trends to preserve user privacy in the course of the Department's enforcement duties. Circle believes that the growth of privacy solutions for digital assets will mirror the development of digital communications privacy, which at its inception was unencrypted and susceptible to easy monitoring. Today, consumers have widespread access to such encryption technologies within their communications systems, and similar privacy-preserving technologies are likely to evolve and be implemented for digital assets as well.

Authorities should promote the use of privacy-preserving technologies as a fundamental component of end user protection even as they continue to enforce robust compliance measures. A partnership based on privacy as a priority will help ensure that new technologies for protecting user privacy also remain compatible with covered entities' AML obligations. For example, ZKPs could help ensure that key details of a suspicious transaction, such as sender, receiver and amount, are available to law enforcement and financial regulators while preventing outside observation. These systems could also be constructed so as to ensure that searches are authorized, or must be done through the presentation of a subpoena or warrant.

The U.S. government should provide clear and transparent guidelines about when it will engage the data of U.S. firms or U.S. persons for blockchain surveillance purposes, as well as the statutory limit of such surveillance activities when they do occur. The Treasury Department should ensure that existing financial privacy protections, such as the 1978 Right to Financial Privacy Act, extend to digital transaction data where applicable. Robust engagement with private blockchain analytics firms and partnerships with industry leaders like Circle may also help with these procedures.

**4. What technological solutions designed to improve AML/CFT and sanctions compliance are being used by the private sector for digital assets? Can these technologies be employed to better identify and disrupt illicit finance associated with digital assets and if so, how?**

Innovations in privacy-preserving digital identity, authentication, and verification are being introduced by Circle and other leading organizations at a rapid pace, with broad implications for AML/CFT and sanctions compliance. As previously noted, Circle is a partner and key contributor to Verite, a set of digital identity standards. Crucially, because identity is verified by an attestation instead of representation of personal information, data sharing and possible leakage is minimized.

Digital privacy solutions like Verite will respect individual privacy and decrease the potential compromise of personal identifying information from cyberattacks, while still providing for robust AML/CFT protocols by reducing the number of unjustified data aggregation repositories maintained through government and private firms. By employing digital identity solutions, VASPs and protocols can ensure that actors using these services are identified in the course of a legitimate investigation. As previously discussed, digital identity solutions may also be used to prevent bad actors from engaging with trustless DeFi protocols in an effort to avoid asset recovery. Circle encourages Treasury to consider rulemaking strategies that incorporate digital identity solutions into existing KYC regulations.

*Zero-Knowledge Proofs*

Novel cryptographic tools such as ZKP technology, currently being developed by the private sector in a number of contexts, have the potential to harmonize consumer privacy and AML/KYC compliance. ZKP technology works by cryptographically proving a relevant piece of information, such as that a user is not a sanctioned or wanted individual, without revealing additional sensitive information to outside observers.

A ZKP system consists of two public algorithms, ZK-Prove and ZK-Verify, that allow the prover and verifier to confirm that an interaction has occurred without the need for intermediaries or revealing the underlying data. Functioning ZKP systems have been built in a number of identity and cryptocurrency contexts and have also been proposed for use in the legal field.[33] With such a system in place, the owner of an address could reveal information to law enforcement or financial regulators, either by request or in response to a subpoena or search warrant, while still safeguarding their privacy. Alternatively, law enforcement could obtain evidence that a third party

[33] Dor Bitan, Ran Canetti, Shafi Goldwasser, and Rebecca Wexler, 2022, "Using Zero-Knowledge to Reconcile Law Enforcement Secrecy and Fair Trial Rights in Criminal Cases" (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4074315).

(such as an exchange) had verified a user's identity as being non-problematic without resorting to direct engagement. Though these technologies have not yet reached scale, Treasury might consider how it can better take advantage of cryptographic systems to ensure AML/CFT compliance when they do enter mainstream adoption.

*TRUST Protocol*

Ensuring compliance among centralized parties will be crucial to enforcing AML/CFT rules as the volume of transactions handled by VASPs grows. As Treasury notes in the National Risk Assessment, "when VASPs fail to register as MSBs with FinCEN or do not implement sufficient AML controls, such as filing SARs or keeping certain records, criminals are more likely to exploit those VASPs without detection."[34] To ensure compliance with financial flows across borders, 35 VASPs partnered together to create the TRUST protocol. The TRUST platform is a means to convey required transmitter information between exchanges in compliance with the Travel Rule. The TRUST platform is an encrypted messaging network which passes required KYC information peer-to-peer between VASPs. As the U.S. government is already involved in regulating centralized entities such as VASPs, this additional solution helps ensure that malicious actors cannot hide behind a screen of anonymity online.

*Other Technologies*

Lastly, enforcement agencies can rely on more advanced location services to pinpoint actors engaged in sanctions evasion. Increasingly accurate geocoding services index the globe with unique keywords, achieving far greater accuracy than a street or IP address. Such systems have already been harnessed by emergency services (including Dallas EMS and Fire) within the United States as well as in Europe, but will need further development to interact with distributed ledger technology transactions.[35] Regulators will also need to integrate these solutions with an eye toward protecting privacy and the fundamental rights of users across international jurisdictions.

**5. Are there additional steps the U.S. Government can take to promote the development and implementation of innovative technologies designed to improve AML/CFT compliance with respect to digital assets?**

The Treasury Department should endeavor to make public and share with industry their assessments of financial technology, such as through reports like those issued under the auspices of the 2020 AMLA Section 6210, which could help the private sector stay compliant and ease the burden of financial monitoring. Similar to the requirements of Section 6210, such reports might require "the Secretary of the Treasury, in consultation with regulators and other relevant parties, to prepare and submit a report assessing the impact of technology on financial crime compliance."[36]

---

[34] Department of the Treasury, 2022, National Money Laundering Risk Assessment, (https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf).
[35] Julia Edinger, 17 October 2022, "Dallas PD, Fire Roll Out Enhanced Call Locator Tech ("https://www.govtech.com/public-safety/dallas-pd-fire-roll-out-enhanced-call-locator-tech).
[36] GuideHouse, 2022, "AMLA 2020 Summary Grid" (https://guidehouse.com/-/media/www/site/insights/financial-services/2021/fs_amlagrid.pdf).

AMLA Section 6101 calls for the Treasury Department to "publish a report outlining AML/CFT policy priorities and requires that ongoing examinations evaluate a financial institution's incorporation of the identified priorities into their risk-based AML/CFT programs."[37] The industry would also benefit from feedback on how public-private collaboration informs regulatory reforms and policy developments. Such information sharing would allow financial institutions to remain in step with Treasury's views and best-practices around AML/CFT, and to make changes to their own protocols when necessary. Additionally, because the private sector is the front line for AML/CFT efforts, increased collaboration and direction from FinCEN specifically on financial technology and policies will help covered institutions embrace the most effective and efficient procedures.

Finally, and as discussed in a prior answer, there are clear incentives for the market to adopt more innovative solutions to verify an individual or entity's identity. Covered entities have been reticent to do so, likely due to the start-up costs associated with incorporating new technology and potential enforcement actions. Treasury and the industry publicly recognize the multitude of benefits from privacy-preserving yet compliant digital identity solutions but have yet to take a more concerted role to encourage adoption. Digital identity is not only an imperative for financial services companies: for instance, the Department of Health and Human Services has recently indicated that digital identity could address problems within the healthcare system, like Medicare fraud. Therefore, the Treasury Department should consider working with other government agencies that might have an interest.

**6. How can law enforcement and supervisory efforts related to countering illicit finance in digital assets better integrate private sector resources?**

While law enforcement and the digital asset industry have begun building partnerships to better facilitate the reporting of illicit financial activity, greater transparency and guidance are still needed around what innovations are permissible and what expertise would help the government better perform its duties. For example, despite cumbersome, expensive, and even outdated traditional methods to conduct KYC processes, the Treasury Department's own research has discovered that financial institutions are hesitant to adopt innovative digital identity technologies due to concerns from federal and state examiners.[38] The Treasury Department should therefore work with the private sector to identify new privacy-preserving identity and verification models that can be widely adopted, in addition to embracing technologies such as digital identity, ZKP technology and the TRUST protocol.

Government agencies and departments might also benefit from exchange programs or "secondments" that embed private sector analysts within government agencies, or vice versa. These temporary positions would allow for crucial knowledge exchange on the use of blockchain analytics and other emerging technologies between the public and private sectors, and increase trust between firms and agencies that will be crucial for countering the use of digital assets for illicit finance. However, it will also be critical for agencies that run these programs to ensure that

[37] Ibid.
[38] FinCEN, 2021, "Innovation Hours Program: Emerging Themes and Future Role in AML Act Implementation" (www.fincen.gov/sites/default/files/2021-03/FinCEN%20IH%20Prgm%20Public%20Report%20508C.pdf)

their core regulatory competencies remain in the hands of civil servants, so as to avoid any possibility of impropriety or corporate capture.

Given that private sector KYC processes are central to an effective AML/CFT program, regulators, law enforcement, and the industry must work together to develop better solutions and take advantage of private sector expertise without running afoul of existing regulations. Indeed, the Department of Justice's report on *The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets* states, "the private sector plays the first line of defense in detecting and monitoring suspicious activity that takes place through their institutions and on their own platforms…financial regulatory agencies use multiple complementary third-party tools to identify, trace, and attribute digital asset transactions on all major and most minor cryptocurrency and stablecoin blockchains."[39]

Law enforcement and financial regulators should work to build relationships with blockchain analytics firms and digital asset issuers to incorporate their know-how and intelligence capabilities into the fight to prevent illicit finance. Recently, Chainalysis took steps to cement these relationships through the National Cyber-Forensic and Training Alliance (NCFTA). Circle recommends that the Treasury Department work to develop similar relationships with analytics firms as well as to cultivate similar capacities in-house.[40]

**7. How can Treasury maximize the development and use of emerging technologies like blockchain analytics, travel rule solutions, or blockchain native AML/CFT solutions, to strengthen AML/CFT compliance related to digital assets?**

In emerging and largely unregulated industries such as the digital assets sector, it is crucial that regulators and law enforcement develop early and reciprocal relationships with private sector actors to share information and combat illicit activity. The White House *Executive Order on Ensuring Responsible Development of Digital Assets* notes that the U.S. government has long been at the forefront of promoting financial innovation in the private sector, but must also "enhance dialogue with the private sector to ensure that firms understand existing obligations and illicit financing risks associated with digital assets, share information, and encourage the use of emerging technologies to comply with obligations."[41] Circle applauds the Treasury Department for moving ahead with this Request for Comment as a means to better cement its AML/CFT guidance and enhance its relationship with private firms.

However, in order to ensure the continued success of such partnerships as well as the efficacy of the U.S. AML/CFT regime, it is crucial that U.S. government agencies avoid regulation by enforcement as a primary means of promulgating new rules for countering illicit finance. Doing so risks damaging the lines of communication between private sector entities and regulators, which are central to combating bad actors in the digital asset economy. For example, recent sanctions

---

[39] U.S. Department of Justice, September 2022, "The Role Of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets" (https://www.justice.gov/ag/page/file/1535236/download).

[40] Example: NCFTA (https://www.ncfta.net/).

[41] The White House, 16 September, 2022, "Fact Sheet: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets" (https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/).

designations raise novel questions about the application of existing regulations and burdens on VASPs and individuals in addressing the risks with decentralized autonomous organizations. Going forward, it should be a priority of the Treasury Department to ensure that all parties are aware of the applicability of current rules and regulations, in order to prevent knock-on effects that can harm other actors in the space. Circle encourages the Treasury Department to work closely with Congress to determine whether additional statutory measures are needed to clarify compliance obligations and AML/CFT reporting requirements for entities involved in the digital assets ecosystem.

**8. How can financial institutions offering digital assets better integrate controls focused on fiat currency and digital asset transaction monitoring and customer identification information to more effectively identify, mitigate, and report illicit finance risks?**

In any emerging technology, the costs of establishing robust compliance programs can be significant – particularly for market entrants – and, as a result, implementation of controls can often lag behind market growth and product development. As noted above, blockchain analytics and digital identity tools offer large potential to more effectively meet compliance demands in the digital asset space while reducing the time and personnel burden on institutions in onboarding customers and conducting ongoing transaction monitoring. Critically, creating regulatory clarity around the use of digital compliance technology as well as the use of third-party compliance tools would likely result in their wider adoption and incentivize their integration earlier in the development cycle of new digital asset products.

Participation in regulatory sandboxes and tech sprints for compliance technology as well as public-private BSA exchanges will play an important role in knowledge-sharing, integration, and the eventual standardization of these tools in a cost-effective and scalable manner. Both authorities and institutions should pay particular focus to the on/off ramps to fiat currency which often represent the choke points for illicit actors seeking to realize the gains of criminal activity. Lastly, there remains an important role that these technologies can play for non-VASP financial institutions which would benefit from blockchain analytic and other tools, for example, during customer onboarding, risk assessment, and geographic monitoring.

**E. Central bank digital currencies (CBDC)**

**1. How can Treasury most effectively support the incorporation of AML/CFT controls into a potential U.S. CBDC design?**

As noted by policymakers, legislators, and technical experts, the decision whether and how to develop and design a CBDC is complex and presents tradeoffs to competing policy objectives. Circle appreciates the thoughtful and methodical approach taken by federal banking regulators as well as the Office of Science and Technology Policy's recent evaluation of technical design choices for a U.S. CBDC.[42] Circle believes that one of the defining factors guiding the development of a CBDC should be the allocation of risk – whether AML/CFT, prudential, or legal – and whether each risk should disproportionately be borne by the public or private sector. With

[42] White House Office of Science and Technology Policy, September 2022, "Technical Design Choices for a U.S. Central Bank Digital Currency" (https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Technical-Design-Choices-US-CBDC-System.pdf).

respect to AML/CFT risk, international standards set by the FATF clearly indicate that a core component of a jurisdiction's AML/CFT regime is ensuring that financial and non-financial reporting entities maintain the burden of identifying, assessing, and implementing their own risk-based AML/CFT programs. Shifting all or even some of that risk burden to the public sector, in addition to the practical challenges of managing compliance for any non-bank customers, could significantly distort that incentive structure and impact adoption of AML/CFT controls. As the U.S. government further researches CBDCs, Circle believes that a guiding principle in the consideration of a CBDC should be the allocation of risk with a strong bias towards maintaining the compliance burden on the private sector.

Circle remains ready to provide further input or comment on the technical considerations of a CBDC and AML/CFT controls – for example, the transport layer, access tiering, identity privacy, security, hardware, transaction privacy, offline transactions, and ledger history – as well as the broader policy issues of identity and transaction privacy.