November 3, 2022

United States Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, D.C. 20220

Re: Ensuring Responsible Development of Digital Assets; Request for Comment on Digital-Asset Related Illicit Finance and National Security Risks

Ladies and Gentlemen:

The Securities and Financial Markets Association ("SIFMA") appreciates the opportunity to respond to the Treasury Department's September 20, 2022 Request for Comment ("RFC") on "Ensuring Responsible Development of Digital Assets" as it pertains to illicit finance and national security risks.[1] SIFMA supports the development of safe, regulated digital asset markets, and are encouraged by the ongoing work that was directed by the Executive Order 14067, "Ensuring Responsible Development of Digital Assets" (hereafter "the Executive Order").[2] This effort, which has already resulted in the publication of several well-considered reports, is an important step towards a better understanding of the evolving digital assets marketplace and its prospects; how responsible innovation can serve and protect investors; and more generally, how the United States can ensure that it retains the same leadership role in digital asset capital markets as it has in the "traditional" capital markets space.

[1] 87 Fed. Reg. 57556 (Sept. 20, 2022), https://www.govinfo.gov/content/pkg/FR-2022-09-20/pdf/2022-20279.pdf.

[2] Exec. Order No. 14067, 87 Fed. Reg. 14143 (Mar. 14, 2022), https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets.

In this letter, we:

- Illustrate how regulated financial institutions (both banks and non-banks, such as our broker-dealer members) are well-positioned to manage the illicit financing risks posed by digital assets;
- Suggest that regulators review existing rules and operating models to best engage with digital assets and blockchain infrastructure;
- Describe how new digital ledger technologies ("DLT") can be employed to help better manage illicit financing risks; and
- And posit that a "wholesale" CBDC ("wCBDC") or alternative which builds on the existing role of regulated financial institutions would allow for better management of illicit financing risks relative to a more widely adopted "retail" ("rCBDC") model.

I. Benefits that Regulated Financial Institutions Bring to the Management of Illicit Financing Risks

As we have noted in recent letters[3], the participation of "traditional" financial services firms, such as regulated banks and broker-dealers, in the digital asset markets offers a broad range of benefits to reduce illicit finance risks and increase transparency.[4] These institutions have a long history of developing and honing Bank Secrecy Act ("BSA") and Combating the Financing of Terrorism ("CFT") compliance programs, including anti-money laundering ("AML") and know-your-customer ("KYC") procedures, and illicit financing controls. Regulated financial institutions have a well-established track record of managing a wide variety of existing and emerging illicit financing risks; there is every reason to believe that they can apply that deep expertise to digital assets. There is also every reason to believe that the mature regulatory frameworks governing illicit financing risks can be applied to digital asset technologies, albeit with modifications that reflect the blockchain technology's unique characteristics.

Regulated financial institutions also provide supervisors and law enforcement with transparency into potential illicit financing activities that they would otherwise lack. Banks and broker-dealers are supervised and examined on an ongoing basis by numerous regulators globally to ensure compliance with illicit financing regulations. Regulators receive periodic reports from the institutions they supervise, and they also have access to information from the examination and onsite supervisory processes and

---

[3] *See*, SIFMA comment letter to Treasury on "Ensuring Responsible Development of Digital Assets," dated Aug. 8, 2022, https://www.sifma.org/wp-content/uploads/2022/08/Ensuring-Responsible-Development-of-Digital-Assets.pdf. *See also*, SIFMA comment letter to the U.S. Department of Commerce on "Developing a Framework on Competitiveness of Digital Asset Technologies," dated July 5, 2022, https://www.sifma.org/wp-content/uploads/2022/07/SIFMA-Response-to-RFC-Developing-a-Framework-on-Competitiveness-of-Digital-Asset-Technologies.pdf.

[4] In this context, "regulated" financial institutions refers to market participants whose activities are overseen by the regulatory and supervisory agencies that govern current capital markets participants, such as banking and prudential regulators, securities and commodities regulators, and self-regulatory organizations ("SROs").

through formal and informal data submissions. As a result, financial regulators and law enforcement authorities can identify bad actors and mitigate a variety of potential national security and criminal threats. It is crucial that equivalent illicit financing requirements and supervision be extended to cryptocurrency centric firms that at present are only subject to either patchwork regulation or no oversight whatsoever. Failure to do so could lead to a dangerous concentration of illicit finance risks in unregulated parts of the market.

Finally, regulated financial institutions have a proven track record of responsible innovation, and new digital asset ventures can draw on such institutions' established and robust frameworks for technology and operational risk management, cybersecurity management, and data protection processes. Indeed, as we discuss below, advanced distributed ledger analysis technology that is increasingly being used by regulated financial institutions may help in the prevention financial crimes.[5] Greater regulated financial institution participation would also increase opportunities to develop digitally native solutions for meeting these requirements for asset types whose current features have raised concerns from policy makers from an AML/KYC perspective. For example, financial institutions may apply their experiences with AML/KYC requirements to develop enhanced due diligence practices.

1. Existing Illicit Finance Oversight Regulation in the Context of Digital Asset Markets

For over 50 years since the Bank Secrecy Act was enacted, regulated financial institutions have built and honed their AML/CFT programs and KYC practices. They have substantial experience implementing risk-based controls adapted to their business models and client base, expertise incorporating new technologies, and resources and talent to implement robust compliance programs, essential to the novel illicit finance risks posed by digital assets. Should they engage in this business, which is contingent on regulatory clarity, financial institutions are already in the best position to deal with illicit finance risks posed by digital assets.

The same cannot be said for new entrants into digital assets market, which may not have the same requirements or expertise to detect, prevent, and report to authorities the threats from digital assets. Policymakers should ensure that illicit finance regulation provides high bar and level regulatory playing field for all financial institutions participating in these markets. They should also look to learn from the leading practices that have been implemented by various state regulators to manage illicit finance risks for digital asset market participants. Globally, it will be essential for Treasury to work with international

[5] Sidley Austin, *Blockchain Tracing: The U.S. Government's Newest Tool to Combat Foreign Crime (May 20, 2022)*, https://www.sidley.com/en/insights/newsupdates/2022/05/blockchain-tracing-the-us-governments-newest-tool-to-combat-foreign-crime (last accessed Aug. 5, 2022).

bodies to develop processes understanding the differences among AML/CFT standards, which exist currently in the traditional finance space.

Specifically with respect to current BSA regulations, we offer some suggestions to assist regulated financial institutions to better understand and deal with these threats.

2. Regulators Should Review Existing Rules and Operating Models to Best Engage with Digital Assets and Blockchain Infrastructure

Just as market participants review how blockchain-based and digital asset infrastructure can enhance the management of illicit financing risks, regulators and policy makers should review existing rules and procedures in light of the unique features of digital assets and their supporting infrastructure. We encourage policy makers to assess both how the definitions and assumptions under existing rules and programs may need reinterpretation to provide effective coverage of digital asset markets, and how existing partnerships with market participants can be made more effective.

For example, the BSA is based on a model in which financial Intermediaries are responsible for obtaining, verifying, retaining, and reporting information to the appropriate regulators about the parties to a given transaction. However, many configurations of digital assets do not require third-party intermediaries, and other digital asset transactions may more closely resemble peer-to-peer transfers of monetary instruments, but with a much higher velocity and cross-border scope. Policymakers should consider how BSA oversight procedures for examination and enforcement can apply in these different operating models.

Similarly, operating models for certain digital asset markets that rely on the role of virtual asset service providers (“VASPs”) should consider how recordkeeping and travel rule obligations that apply to banks and traditional money transmitters can be applied to VASPs. These may include issues such as the application of the Funds Recordkeeping rule to transactions between hosted and unhosted wallets, as well as the application of the Funds Travel Rule to transactions between wallets hosted at VASPs.

There may also be definitional changes necessary considering the characteristics of digital asset markets. For example, the typologies that define fraud and other illicit finance activities are based on activities in the traditional finance markets; it is important to assess if adjustments are necessary in the context of digital asset markets .

Policymakers should also consider how certain operating procedures can be changed to better support market participants in managing illicit financing risks for digital assets. For example, information sharing with market participants supports more effective surveillance. As digital asset infrastructure matures, regulators and enforcement agencies could explore benefits of developing the capability to "airdrop"

supervisory notices to digital wallets. In addition, if Suspicious Activity Reports ("SARs") were specifically connected to digital assets, FinCEN could alert the industry of certain trends or risks through its periodic studies.

There may also be areas where the federal protections for regulated entities that take part in voluntary information sharing can be expanded and clarified. This is particularly the case as new technology models, such as those described above, can offer new ways of sharing illicit finance monitoring information more broadly – provided they can be accommodated under regulatory frameworks. For example, Section 314B of the USA PATRIOT Act permits financial institutions, upon providing notice to the Treasury Department, to share information with one another to identify and report to the federal government activities that may involve money laundering or terrorist activity. However, the statute does not contain a clear safe harbor from the consequences of a good faith exchange of information that, in the final analysis, does not involve money laundering or terrorist activity.

3. DLT Infrastructure Can Offer New Possibilities to Manage Illicit Finance Risks

As digital asset markets and blockchain based infrastructure develop further, they have the potential to offer new ledger-based tools to better track client and transaction information to manage illicit finance risks.

In contrast to disintermediated peer to peer crypto markets, where holders can send assets to any other holders on the network, regulated institutions are exploring models where pre-approvals and regulatory checks are needed before any transfer of digital assets. Digital asset infrastructure developed by regulated financial institutions will place these controls at the forefront given existing regulatory frameworks – in contrast to the development of operating models outside the regulatory perimeter. For example, a trust mechanism can be built into the network to provide checks for legal and regulatory concerns, including AML/KYC and sanctions issues. This may or may not be a third party, depending on network configuration. These functions can be overlaid across the existing securities lifecycle, such as issuance, trading, and funds and asset transfer to provide the levels of oversight and control over these functions and their participants as are found in "traditional" markets and infrastructure.

While these technological solutions offer the potential for enhanced illicit finance risk monitoring, they are still a work in progress as new infrastructure and supporting technologies develop and, importantly, as protocols for market participants using the technologies are developed. There may be some markets where technological solutions cannot provide full mitigation of illicit financing risks, particularly in unhosted or self-hosted transactions. As these markets evolve, they will need to balance issues, such as the identify and role of validators, and buy-in from participants.

At a high level, there are a broad range of tools that can be built into the infrastructure for digital asset markets to manage illicit financing risks. Identity registrars and oracles on behalf of an issuer or other market participants could conduct due diligence and be responsible for keeping records of digital asset holders' identities. These information sources could combine information which is input natively on a blockchain with references to other information sources which are off-chain, such as existing KYC/AML databases. Smart contracts could incorporate a whitelisting process for participants' identities, as well as connecting on-chain whitelisting to allow for rapid approval of transactions without needing to request this information from a registrar.

We encourage Treasury to work closely with the private sector – both financial institutions and infrastructure and technology providers – to understand how emerging technology can support our shared goals of providing AML / KYC oversight. Similarly, regulated financial institutions can and should support policymakers' efforts to deploy the latest innovations in blockchain-based forensic technology in combatting illicit finance. SIFMA is happy to discuss with Treasury the potential application of these technologies.

4. Central Bank Digital Currencies and Leveraging Existing Regulated Financial Institution Oversight

We believe it is essential for policy makers to understand the implications of a digital dollar on the broad range of regulations, processes, and products before making any decision on a U.S. CBDC. We encourage Treasury to refer to our prior submissions for a broader discussion of SIFMA's positions on the broader questions around a potential U.S. CBDC, its impacts on the capital markets, and key design considerations.[6]

The distinction between wholesale and retail CBDCs ("wCBDCs" and "rCBDCs") has important implications for policymakers as they consider how to mitigate potential illicit finance risks of a future digital dollar. A wCBDC would likely offer many advantages in terms of managing illicit finance risk compared to a rCBDC, both in terms of its ability to leverage existing industry controls and obviating the need for controls related to the broader access the rCBDC offers.

wCBDCs would operate on a model of restricted access, where access is limited to qualified financial institutions, similar to the restrictions on access to central bank money today. There are different potential models for the types of institutions that would have wCBDC access – such as some combination of

[6] *See*, SIFMA comment letter to the Federal Reserve Board re: "Money and Payments: The U.S. Dollar in the Age of Digital Transformation," dated May 20, 2022, https://www.sifma.org/resources/submissions/cbdc-discussion-paper-response/

prudentially regulated banking organizations, a limited number of non-bank, regulated payment systems providers, and potentially other, non-bank market participants under some type of rules and oversight. wCBDC access would restrict participation to regulated financial institutions and therefore obviate the challenges associated with widespread retail access to an rCBDC.

As discussed above, regulated financial institutions are already compliant with a range of AML / KYC, and illicit finance control regulations, and have robust procedures in place to meet these requirements. By restricting CBDC access to these institutions, any illicit finance controls specific to a CBDC can be layered upon these existing frameworks for control and disclosure. While there may be areas where a wCBDC will introduce new concerns that are not covered by existing regulations on financial institutions, policymakers can focus on specifically addressing these gaps as opposed to developing entirely new frameworks for managing illicit finance risk.

In contrast, rCBDCs with widespread adoption across the general public could present a range of challenges if policymakers wish to embed robust illicit finance controls within the program. This is particularly the case given the competing concerns around preserving the privacy of rCBDC users.

For these and other reasons, while we are not yet able to opine on the desirability of adopting a U.S. CBDC, we do believe that if policymakers were to move forward with adoption at some future point, the primary focus should be on wCBDC.

However, policymakers' analyses of the viability of any CBDC operating model should include a careful review of whether the goals of a wCBDC might best be accomplished through regulated commercial models which are already available or under development. Analysis should cover a broad range of models which could meet the objectives that policymakers seek to achieve through a potential digital dollar. For example, these could include various systems of private tokens, regulated private digital forms of money such as blockchain based deposits, stablecoins or tokenized deposits.[7] Other potential solutions include Partior, a shared-ledger multi-currency clearing platform that can be transacted 24x7x365 and can utilize smart contracts, or the Regulated Liability Network (RLN) proposal to tokenize central bank, commercial bank, and electronic money on the same chain.[8] Policymakers should explore if and how these alternative technology configurations could meet the objectives of a wCBDC, such as the instant movement of value 24/7 either domestically or internationally, integrated into other digitized

[7] Examples of blockchain based deposit products include the JPMCoin (for further information, visit https://www.jpmorgan.com/onyx/coin-system.htm).

[8] Partior is currently live with digital M1 (deposit liabilities of a commercial bank) being provided by JP Morgan (USD) and DBS (SGD). Over time, the platform intends to cover a broad set of currencies and multiple providers for each currency. For further information, visit https://www.partior.com/.

See, The Regulated Liability Network (RLN) Whitepaper, https://www.citibank.com/tts/insights/articles/article191.html.

processes, and serve as “programmable money” insofar as payments can be automated or made conditional on events.

These regulated commercial models would be operated by financial institutions that are already covered by the broad range of AML / KYC controls discussed above. As with wCBDCs, understanding and controlling the illicit finance risks associated with new forms of digital money movement infrastructure will be easier when they build on the roles of regulated market participants.

Regardless of the ultimate operating model for any new digital payments infrastructure, whether CBDC-based or another model, it would need to deliver levels of identity verification and monitoring which are equivalent to private sector oversight functions under existing regulatory frameworks, consistent with the principle of “same activity, same risk, same regulatory outcome.” Similarly, policymakers should ensure any new technology (whether a CBDC-based model or an alternative) should not unintentionally be advantageous to or encourage illicit financial activity.

****

We appreciate the opportunity to respond to this Request for Comment. On issues such as the role of regulated financial institutions in digital asset markets and the considerations around a potential U.S. CBCD, we encourage the Treasury Department staff to refer to the SIFMA comment letters and position papers cited in this letter, which provide a more in-depth exploration of these issues and our members’ perspective on them.

Please do not hesitate to reach out to Charles De Simone, Managing Director, Technology and Operations (cdesimone@sifma.org), Peter Ryan, Managing Director and Head of International Capital Markets and Strategic Initiatives, (pryan@sifma.org), Bernard Canepa, Managing Director and Assistant General Counsel (bcanepa@sifma.org), or me with any questions or to discuss further.

Sincerely,

Kenneth E. Bentsen, Jr.
President and CEO
Securities Industry and Financial Markets Association
1099 New York Ave., N.W. 6th Floor

Washington, D.C. 20005
202-962-7400
202-215-8596 (cell)
kbentsen@sifma.org