September 28, 2022

Skadden

The Distributed Ledger

Blockchain, Digital Assets and Smart Contracts

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

Treasury and Justice Department Reports Signal Tougher Enforcement and Regulation in the Digital Assets Sector

On September 16, 2022, the U.S. Department of the Treasury and Department of Justice released four much-anticipated reports on different aspects of cryptoasset regulation. They confirm the Biden administration's broad but cautious support for innovation in this area and, at the same time, actively support assessing the risks of digital assets and pursuing responses.

The reports recommend that both departments make civil and criminal enforcement in the digital assets area a high priority, in order to protect consumers and markets, and to prevent illicit activities. They also advocate that the U.S. government take a leading role in standard-setting regarding illicit activities at the international and state level.

The reports do not, as some hoped, articulate a broad regulatory framework for digital assets and, indeed, they articulate few specific legislative or regulatory reforms. Instead, the documents reflect the administration's incremental approach to regulating and stimulating development of the new technology.

Overview and Key Takeaways From the Reports

Three of the reports were issued by the Treasury Department:

- "The Future of Money and Payments" (Payments Report)
- "Crypto-Assets: Implications for Consumers, Investors and Businesses" (CIB Report)
- "Action Plan to Address Illicit Financing Risks of Digital Assets" (Illicit Finance Report)

The Department of Justice released the fourth:

- "The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets" (DOJ Report)

All four reports were mandated by President Biden's March 9, 2022, "Executive Order on Ensuring Responsible Development of Digital Assets" (EO 14067). Like EO 14067, the reports generally welcome innovation and broadly accept digital assets as a component of the U.S. financial system, but focus on the potential risks of digital assets rather than the benefits they may provide. Among other things, the reports raise concerns about consumer protection, illicit finance and potential gaps in the current regulatory regime, particularly relating to novel products and services like decentralized finance (DeFi) and non-fungible tokens (NFTs).

Significant issues touched on in the reports include:

CBDC. The Payments Report questions the near-term need for a U.S. central bank digital currency (CBDC), particularly in light of alternative near-real-time payment systems like FedNow, which is being developed by the Federal Reserve. Treasury recommends further study of the risks and benefits of a CBDC, suggesting one is not imminent in the U.S. While the Payments Report highlights risks related to stablecoins, it does not provide any new insights about the administration's approach to their regulation.

Unbanked and underbanked populations. The CIB Report reflects on the balance between the potential benefits that digital asset technologies can offer to unbanked and underbanked populations and the risks they pose to those groups. These groups stand to benefit from the new technology, but also could be highly vulnerable to misuses of it, the report says. It recommends that relevant agencies expand monitoring and enforcement efforts, issue clearer and more practical guidance, and educate the public about digital assets to ensure that the benefits of these technologies outweigh the risk they pose to consumers, investors and businesses.

Money-laundering and terrorism financing risks. The reports emphasize the risks digital assets pose for U.S. and international anti-money laundering (AML) programs and efforts to counter the financing of terrorism (CFT), and recommend actions to clarify and strengthen enforcement of existing AML/CFT laws and regulations. The Illicit Finance Report and the DOJ Report strongly suggest that the agencies view digital assets as a key enforcement priority and will seek additional resources in the near term to address threats. The Illicit Finance Report also emphasizes the importance of U.S. leadership on the global stage, multilateral cooperation and the adoption of robust global regulatory standards for the digital asset sector.

The Illicit Finance Report cites mixing services, dark net markets and non-compliant virtual asset service providers (VASPs) used to facilitate money laundering as specific areas of concern.

Regulatory and procedural reforms. While the reports do not advocate for significant legislative or regulatory reforms, the DOJ Report recommends amendments to some bank secrecy and money transfer laws so they clearly apply to digital assets. It also suggests changes to venue rules and statutes of limitations in digital-assets cases.

Overall approach. While the Illicit Finance Report does not alter current regulatory obligations, it does suggest what the Treasury Department is contemplating with respect to the regulation of digital assets and supervision of related stakeholders. It also discloses that the Treasury Department will issue two new risk assessments next year related to DeFi and NFTs.

Beyond pushing for near-term action on the enforcement front, however, the reports strike a cautious and measured tone. Both the Treasury Department and the Justice Department call for using — and bolstering — their existing authority to promote consumer protection and combat illicit finance related to digital assets, even as they seek modifications and expansions of those powers in the future. But the reports do not suggest that significant legislative or regulatory changes are imminent, such as a comprehensive regulatory framework for digital assets.

Payments Report: The Future of Money and Payments

The Payments Report builds upon the Federal Reserve's January 20, 2022, discussion paper, "Money and Payments: The U.S. Dollar in the Age of Digital Transformation," and is part of a broader dialogue between the Treasury Department, Federal Reserve and various stakeholders regarding the prospect of a Federal Reserve-backed CBDC.

The report acknowledges that a U.S. CBDC could offer certain benefits, potentially providing for a faster, more efficient payment system, facilitating cross-border payments and expanding financial inclusion. But the report does not appear to view the adoption of a U.S. CBDC as an urgent matter, arguing, for example, that the primacy of the U.S. dollar is unlikely to be displaced by foreign CBDCs. Moreover, the report cautions that a CBDC would present operational challenges, including compliance with AML/CFT laws and regulations and give rise to risks, including potential runs on U.S. CBDC in times of stress that could lead to financial instability.

According to the report, a CBDC could be a target for hackers and would have to be extremely resilient and reliable. The report does not stake out a position on whether the benefits of a U.S. CBDC outweigh the risks, and recommends that the Federal Reserve and other U.S. government stakeholders continue to advance work on the digital currency in case it is later determined to be in the national interest — a process that could take years.

Counterbalancing the potential need for a CBDC, the report notes that there are efforts underway to develop real-time payment systems, like FedNow, that are capable of handling higher volumes of transactions at a lower cost than some current payment systems, but without the potential risks of a CBDC. The report recommends that the U.S. government continue to encourage the use of instant payment systems to support a more competitive, efficient and inclusive U.S. payment landscape, in line with the administration's policy goals.

The report observes the increasing role of nonbanks in providing payment services, saying that their participation may increase competition, inclusion and innovation, benefiting consumers. However, if these firms are not adequately regulated

and supervised, there may be risks to consumers, the financial industry and the broader economy. The report recommends a federal framework for payments regulation that would protect users and the financial system, while supporting responsible innovation. Such a framework could help realize the benefits from nonbank payment providers while minimizing risks and could provide a pathway for nonbanks to participate directly in instant payment systems.

Finally, the report emphasizes that the U.S. has a strong national interest in being at the forefront of technological developments in the payment field and in supporting global standards for cross-border payment systems that reflect U.S. values (including privacy and human rights), are consistent with AML/CFT goals and protect U.S. national security. The report emphasizes that the U.S. is already active in efforts to improve cross-border payments, including through the G20, the Financial Stability Board and the Committee on Payments and Market Infrastructure. The U.S. should use its leadership position internationally to prioritize efforts to improve cross-border payments, both to enhance payment system efficiency and protect national security.

CIB Report: Implications for Consumers, Investors and Businesses

Like the Illicit Finance Report, the Treasury's CIB Report provides an overview of blockchain technology, the benefits that it can bring to the unbanked and underbanked, and the various risks that these financial services can present.

It goes on to recommend that relevant agencies adopt a multipart approach to addressing these risks. This should prioritize the need for action to protect consumers, investors and businesses, while legislation on cryptoassets is being debated.[1] The key theme of the CIB Report is that, while cryptoassets may offer certain benefits to the unbanked and underbanked population, this potential user group needs to be protected from the risks presented by what is, at present, a largely unregulated industry. The CIB Report makes three specific recommendations:

- U.S. regulatory and law enforcement agencies should vigilantly monitor the cryptoasset sector for unlawful activity, aggressively pursue investigations and continue to bring civil and criminal actions to enforce applicable laws with a particular focus on consumer, investor and market protection. This includes expanding and increasing investigations and enforcement, particularly of unfair, deceptive or abusive practices, and improving coordination across agencies.
- U.S. regulatory agencies should continue using their existing authorities to issue "plain language" supervisory guidance and rules to address risks in cryptoasset products and services for consumers, investors and businesses. Agencies should work collaboratively to promote consistent and comprehensive oversight.
- U.S. authorities should work individually and through the Financial Literacy and Education Commission (FLEC) to ensure that U.S. consumers, investors and businesses have access to trustworthy information on cryptoassets.

Uses and Opportunities for Cryptoassets

Before exploring the risks of cryptoassets, the CIB Report outlines some of the uses and opportunities for this technology, grouped into three broad categories:

- cryptoasset-based alternatives to traditional financial products and services;
- financial market and payment system infrastructures; and
- potential for other consumer and commercial uses (*e.g.*, NFTs, gaming, records, identity, supply chain management).

Among the benefits cited are:

- improving efficiency and speed, and reducing the cost of international payments and remittances by addressing the lack of interoperability between payment infrastructures in different countries;
- improving the provision of trade credit and other administrative processes related to trade by creating a single source of reference information to help participants synchronize the movement of physical goods, information and financing;
- creating new payment streams for employees and businesses, especially among the unbanked and underbanked;
- creating a real-time settlement process; and
- creating faster and cheaper transactions, increased transparency of asset positions and increased liquidity through fractionalization.

Risks and Exposures for Consumers, Investors and Businesses

The CIB Report devotes much of its analysis to the risks posed by cryptoassets, which it divides into three categories: (1) conduct risks such as theft and fraud; (2) operational risks that are specific to blockchains; and (3) risks arising from cryptoasset intermediation. Examples cited include:

[1] The CIB Report defines "crypto-assets" as "all types of representations of value or claims in digital form that rely on the use of a method of distributed ledger technology, excluding central bank digital currencies (CBDCs)."

Conduct Risks

- **Fraud, theft and mismanagement.** The CIB Report notes that the volume of fraud, scams and thefts in the blockchain ecosystem was at an all-time high in 2021, with scams being the most prevalent form of malicious activity. Blockchain technology has unique features that make it attractive for unlawful activity of this kind, the report states, including the ongoing evolution of the technology, pseudonymity, the irreversibility of transactions and the current asymmetry of information between issuers and consumers. In addition to theft resulting from malicious activities such as phishing, some theft arises from the exploitation of flaws in the smart contract code.
- **Information asymmetry.** A key distinction between traditional capital markets and the cryptoasset ecosystem, the CIB Report notes, is that statutes and regulations establish a robust disclosure regime for traditional markets, providing consumers and investors with material information so they can make informed decisions. In the cryptoasset ecosystem, by contrast, issuers and platforms may not be complying with these requirements, leading to a lack of disclosure standardization, and in some cases a failure to disclose key material information that is essential to assessing risk. This may include a lack of information about important conflicts of interest that founders and initial investors may have, a lack of information on how governance tokens are allocated and how decentralized the platform really is.
- **Platform access.** The CIB Report highlights that, because most blockchain-based projects lack anyone playing a "gatekeeping" role, there is a risk a user could get involved in a platform engaging in unlawful activity.
- **Market manipulation.** Although blockchain-based platforms are transparent, the CIB Report notes that the pseudonymity offered by these platforms means that there is a higher degree of risk of market manipulation and wash trading.

Operational Risks

The CIB Report defines operational risk as the risk of loss caused by flawed or failed processes, policies, systems or events.

- **General features and decentralized governance.** One of the benefits of blockchain technology, the immutable and publicly viewable "smart contract" code on which many platforms operate, is also a risk, the CIB Report notes, since it allows malicious actors to identify and exploit vulnerabilities in the code.
- **Security and scalability tradeoffs.** The CIB Report highlights the fact that issues with scalability of public blockchains can lead to unpredictable, volatile and regressive fees imposed on users.
- **De-anonymization.** While users of Web3 technology tend to be pseudonymous, the transparency of transactions means that, once a user is identified, it is possible to see all their transactions, the CIB Report notes.
- **Mining risks.** While blockchains are, in theory, decentralized, a concentration of miners has made them somewhat centralized in reality. This can be true for proof-of-work systems, and even in a proof-of-stake environment, where staking is concentrated in a few players. The CIB Report also notes that in many consensus mechanisms, miners can observe, select and reorganize transactions, allowing them to prioritize transactions that pay higher fees. This can allow for front-running and market manipulation.

Risks in Cryptoasset Intermediation

- **Resource and capabilities risks.** The high volatility in the price of cryptoassets means that there is an increased risk of margin calls on cryptoasset intermediaries, and follow-on collateral liquidation if margin calls cannot be met. In addition, because many of these platforms are not regulated, there may not be capital and liquidity buffers to absorb and limit the impact of significant events.
- **Custody risks.** The CIB Report notes that there is no comprehensive regime to protect consumers and businesses in the event that a cryptoasset custodian has an insolvency event. These providers may also comingle customer funds with their own.

Opportunities and Risks for Populations Vulnerable to Disparate Impacts

The CIB Report acknowledges that many of the benefits highlighted above are especially important for the unbanked and underbanked populations, such as expanded access to financial services, reduced transaction costs and new ways to build wealth. However, this same population faces unique risks when engaging with cryptoassets, including market volatility, inadequate disclosures, targeted marketing from celebrities and athletes, frauds, scams and surveillance risks, the CIB Report states.

Illicit Finance Report: Proposed Actions

The Treasury's Illicit Finance Report builds on the U.S. government's May 2022 National Strategy for Combatting Terrorist and Other Illicit Financing (National Strategy), which was, in turn, informed by the Treasury Department's 2022 National Risk Assessments on money laundering, terrorist financing and proliferation financing (Risk Assessments). The Illicit Finance Report assesses the risks, observations, and regulatory and enforcement priorities developed in the National Strategy and the Risk Assessments and the "significant illicit financing risks" that digital assets pose.

The Illicit Finance Report follows several notable enforcement and targeting actions by the Treasury Department, including the imposition by the Office of Foreign Assets Control (OFAC) of blocking sanctions on Tornado Cash for its alleged use as a means to launder the proceeds of notable cryptocurrency heists in recent years. (See our August 2022 note, "Treasury and New York Enforcement Actions Reveal Continued Focus on the Cryptocurrency Industry and Regulators' Priorities.") This designation of a decentralized protocol has led some to question whether OFAC overstepped its authority by, in effect, sanctioning a piece of code. (Six Ethereum blockchain users who used Tornado Cash have challenged the action in a suit in federal court in Texas.)

The report highlights seven priority actions and numerous supporting actions to which the U.S. government is committed in its efforts to combat the illicit financing risks associated with digital assets. Not every action highlighted is new; rather, the majority of the actions are intended to "continue and deepen" ongoing work by the Treasury Department.

Monitoring Risk and Revising the Bank Secrecy Act and AML Frameworks

Priority Action 1, "Monitoring Emerging Risk," and Priority Action 3, "Updating Bank Secrecy Act Regulations," as their names suggest, involve ongoing monitoring of emerging and evolving risk in the digital asset space and using the fruits of those efforts to update the U.S. Bank Secrecy Act (BSA) and AML regulatory framework. Priority Action 1 describes using existing BSA reporting channels, the U.S.'s leading role at the intergovernmental Financial Action Task Force, and supporting ongoing research and development to support these goals.

Notably, Priority Action 1 also signals that the Treasury Department will issue a risk assessment of the money laundering and terrorist financing risks related to DeFi conduct by February 24, 2023, and a risk assessment of NFTs by July 2023.

International and U.S. Domestic Coordination and Standardization

Priority Action 2, "Improving Global AML/CFT Regulation and Enforcement," and Priority Action 4, "Strengthening U.S. AML/CFT Supervision of Virtual Asset Activities," express the Treasury Department's intent to foster increased multilateral cooperation — both among international regulatory authorities and at the U.S. federal and state levels — in the regulation of digital assets. The stated goals, both on the global stage and domestically, are to increase engagement and information-sharing among regulators, adopt common standards for licensing and regulating VASPs, and promote more robust and effective supervision through examination and enforcement.

Increased Enforcement and Related Activities

Priority Action 5, "Holding Accountable Cybercriminals and Other Illicit Actors," reiterates that the U.S. government will continue to target illicit actors and the abuse of digital asset technologies through various forms of enforcement activity, including criminal and civil actions, targeted sanctions designations, the issuance of special measures under Section 311 of the USA PATRIOT Act and other means. Priority Action 5 highlights several targets of particular concern, including mixing services, dark net markets and non-compliant VASPs used to facilitate money laundering.

Private Sector Engagement

Finally, Priority Action 6, "Engaging with the Private Sector," forecasts several methods of future engagement with the private sector on digital asset-related risk. These methods include the publication of guidance, advisories and other public documents; participation in private sector events; and the organization of government-sponsored events, such as Financial Crimes Enforcement Network (FinCEN) exchanges and roundtables. Priority Action 7 addresses the development and promotion of an efficient, transparent and effective U.S. payments system. Much of its substance is addressed above in the discussion of the CIB Report.

Next Steps

The Illicit Finance Report concludes with a list of questions and topics for ongoing discussion with international partners and the private sector. These questions and topics cover much of the same ground as the priority actions themselves and were included in a September 20, 2022, request for comment by the Treasury Department. At a minimum, the Illicit Finance Report and the recently issued request for comment demonstrate that the Treasury Department's work in addressing the illicit finance risks presented by digital assets is far from complete.

DOJ Report: Digital-Asset Crimes

The DOJ Report discusses the manner in which illicit actors are exploiting digital assets and the initiatives that the Department of Justice and other law enforcement agencies have established to more effectively detect, investigate and prosecute digital-asset crimes. Most importantly, however, the DOJ Report sets forth recommended regulatory and legislative actions to further enhance law enforcement's ability to address such crimes, as discussed below.

Concurrent with the report's publication, the Justice Department announced the establishment of the nationwide Digital Asset Coordinator Network. The network comprises over 150 designated federal prosecutors from U.S. Attorneys' offices nationwide

and the department's litigating components, and will serve as the department's primary forum for prosecutors to obtain and disseminate training, technical expertise, and guidance about the investigation and prosecution of digital asset crimes.

Priority Proposals

The DOJ Report identifies three priority proposals that are critical to the continued success of prosecutions in the digital assets space:

- extending to VASPs that operate as money services businesses the existing prohibition against tipping off suspects to ongoing investigations that applies to traditional financial institutions;
- strengthening the federal law prohibiting operation of an unlicensed money transmitting business by increasing the law's penalties and clarifying that the statute applies to platforms that enable users to transfer digital assets in a manner analogous to traditional money transmitting businesses, even if no custody or control is assumed over the value to be exchanged; and
- extending the statute of limitations for crimes involving digital assets from five years to 10, and providing for a longer tolling period where the U.S. government has requested foreign evidence, to account for the complexities of digital assets-related investigations.

Proposals To Facilitate Evidence Gathering and Strengthen Penalties

The DOJ Report also recommends legislative and regulatory changes, as well as international cooperation initiatives, to facilitate the gathering of evidence of crimes involving digital assets. Additionally, to facilitate the prosecution of digital assets-related crimes that harm Americans, the department proposes changes to relevant venue provisions that would permit prosecution in any district where the victim or other cybercrime is found. The DOJ Report also proposes to expand existing authorities for forfeiture actions where appropriate in digital assets cases and to strengthen the Federal Sentencing Guidelines applicable to certain BSA violations.

Proposals Concerning BSA Regulations

The DOJ Report further recommends that FinCEN issue a final rule stemming from its October 2020 proposed rulemaking, which would amend the recordkeeping and travel rule regulations under the BSA. Among other things, that rule would clarify that such regulations apply to transactions above the applicable threshold involving convertible virtual currency, as well as transactions involving digital assets with legal tender status. The department also supports the application of the BSA — including the obligation to implement an AML/CFT compliance program and report suspicious transactions to regulators — to NFT platforms, including online auction houses and digital art galleries.

Proposal To Ensure Adequate Funding of Law Enforcement

The Justice Department recommends ensuring that law enforcement and regulatory agencies receive the resources required to conduct, and staff, technologically sophisticated and data-driven digital assets-related investigations.

Conclusion

After 180 days of study, the Biden Administration has published nine reports pursuant to EO 14067, including the four described in this alert. A tenth report, expected soon from the Financial Stability Oversight Council, is expected to address financial stability risks associated with digital assets and to identify any federal regulatory gaps that may exist in supervision and regulation.

To date, however, the administration has not made specific legislative requests or proposals to the current Congress. If it does not do so in 2022, it will have to engage with a new Congress that may not share its philosophy or regulatory inclinations, although so far many of the legislative proposals in the digital asset sphere have been bipartisan.

The administration is likely to continue its cautious and incremental approach to digital assets. The next six months are likely to be dominated by continued study and interagency collaboration on guidance and enforcement actions. The Treasury Department's risk assessments of DeFi and NFTs next year will be of particular interest. We expect the administration to continue to monitor digital asset developments, assess potential risk to the financial system, address misuse and misapplication of technology to evade U.S. laws and harm consumers, and evaluate the threats and risks to the U.S. dollar and the ability of the U.S. to maintain a dominant position in global finance.

Contacts

Jamie L. Boucher
Partner / Washington, D.C.
202.371.7369
jamie.boucher@skadden.com

Alexander C. Drylewski
Partner / New York
212.735.2129
alexander.drylewski@skadden.com

Alessio Evangelista
Partner / Washington, D.C.
202.371.7170
alessio.evangelista@skadden.com

Eytan J. Fisch
Partner / Washington, D.C.
202.371.7314
eytan.fisch@skadden.com

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Jessie K. Liu
Partner / Washington, D.C.
202.371.7340
jessie.liu@skadden.com

Daniel Michael
Partner / New York
212.735.2200
daniel.michael@skadden.com

Sven G. Mickisch
Partner / New York
212.735.3554
sven.mickisch@skadden.com

Bao Nguyen
Partner / Washington, D.C.
202.371.7160
bao.nguyen@skadden.com

Khalil N. Maalouf
Counsel / Washington, D.C.
202.371.7711
khalil.maalouf@skadden.com

James E. Perry
Associate / Washington, D.C.
202.371.7652
james.e.perry@skadden.com

Joseph M. Sandman
Associate / Washington, D.C.
202.371.7355
joseph.sandman@skadden.com

Greg Seidner
Associate / Washington, D.C.
202.371.7014
greg.seidner@skadden.com

Joel S. Thompson
Associate / Washington, D.C.
202.371.7561
joel.thompson@skadden.com

Javier A. Urbina
Associate / Washington, D.C.
202.371.7376
javier.urbina@skadden.com