Davis Polk

Treasury Department and Department of Justice signal further regulation of digital asset industry

September 29, 2022 | Client Update | 16-minute read

The U.S. Treasury and Justice Department released regulatory and legislative recommendations and priorities to address illicit finance risks connected to the digital assets ecosystem, following President Biden's executive order on the regulation of digital assets.

On September 16, 2022, the U.S. Department of the Treasury (the "Treasury Department" or "Treasury") and the Justice Department (DOJ) released reports setting out the agencies' respective legislative, regulatory, and policy recommendations and priorities on the regulation of digital assets. Earlier this year, the Biden Administration signaled its intention to regulate the digital asset industry, releasing Executive Order 14067, which reinforces the United States' commitment to shaping the development of the digital assets industry. As previewed in our client update on Executive Order 14067, President Biden mandated multiple reports on six principal themes, which included mitigating illicit finance and national security risks posed by the misuse of digital assets. Specifically, Executive Order 14067 calls for the development of a coordinated interagency action plan for mitigating the digital?asset?related risks identified in the National Strategy for Combating Terrorist and Other Illicit Financing (the "Illicit Financing Strategy").[2][1]

Section 5(b)(iii) of Executive Order 14067 directs the Attorney General to issue a report on "the role of law enforcement agencies in detecting, investigating, and prosecuting criminal activity related to digital assets," which must include recommendations on regulatory and/or legislative actions. On September 16, 2022, the DOJ issued its report, entitled the "Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets" (the "DOJ Report").[3]

The DOJ Report offers specific changes to laws and regulations that would expand the scope of the Bank Secrecy Act (BSA) and other laws, clarify the application of those laws to virtual asset service providers (VASPs) – including VASPs acting as money services businesses (MSBs) – and toughen penalties for violations of those laws. The DOJ further recommends extending BSA requirements to non-fungible tokens (NFTs). However, legislative changes to enact those recommendations are at best uncertain in the current environment and, to the extent that the DOJ's recommendations require it, the Financial Crimes Enforcement Network (FinCEN) is unlikely in the short-term to implement such changes, given competing priorities and their staffing and resource challenges.

Pursuant to Section 7(c) of Executive Order 14067, the Treasury Department also published its "Action Plan to Address Illicit Financing Risks of Digital Assets" on September 16, 2022 (the "Illicit Finance Action Plan" or the "Action Plan"). The Action Plan identifies priority and supporting actions to support the U.S. government's commitment to combatting the illicit finance risks identified in the Illicit Financing Strategy. The priority actions identified in the Action Plan include monitoring risks, working with international partners to improve cooperation on and implementation of international AML standards, strengthening U.S. AML regulations and operational frameworks, and improving private sector compliance and information sharing.

Finally, the Treasury Department issued a Request for Comment (RFC) to gather feedback on the illicit finance and national security risks posed by digital assets. The RFC was issued pursuant to Executive Order 14067 and the Illicit Finance Action Plan, and comments on the RFC are due by November 3, 2022.

The DOJ Report and recommendations

Consistent with the requirements of Executive Order 14067, the DOJ Report presents the Justice Department's view of the role of law enforcement in investigating and prosecuting criminal activity related to digital assets and recommends certain regulatory and legislative actions to facilitate the efforts of law enforcement agencies. As required under Executive Order 14067, the DOJ Report also addresses the methods through which illicit actors exploit digital assets. Of the areas covered by the DOJ Report, however, the Justice Department's proposed regulatory and legislative actions are perhaps the most noteworthy (and substantively new).[4]

Contemporaneous with its release of the DOJ Report (and underscoring the DOJ's heightened focus on digital assets), the Justice Department also announced the creation of the Digital Asset Coordinator (DAC) Network, a taskforce comprised of 150 federal prosecutors that will serve as the Criminal Division's primary forum for training, technical expertise, and guidance on the investigation and prosecution of digital asset crimes.[5]

Recommended regulatory and legislative actions

The DOJ Report proposes a variety of regulatory and legislative actions that the Justice Department believes "would facilitate efforts to investigate, prosecute, and otherwise disrupt digital assets-related criminal activity." The DOJ's recommendations cover a range of areas, including, among other things, the expansion of criminal statutes applicable to MSBs to cover certain VASPs, amending the BSA to cover NFTs, and legislative changes to enhance the DOJ's evidence-gathering and forfeiture authorities. If enacted, these proposals would clarify application of existing laws to the digital assets industry and enhance the penalties for violations of applicable laws.

The DOJ Report highlights three "priority proposals" that the Justice Department believes to be "integral to the continued success of prosecutions and other disruptions in the digital assets space." These include:

> **1. Expanding to virtual asset service providers the laws preventing employees of financial institutions from tipping off suspects to ongoing investigations.** The DOJ notes that the federal statutes prohibiting officers or agents of financial institutions from notifying customers when their records are sought via grand jury subpoena and certain other subpoenas do not currently cover VASPs that act as MSBs because those entities fall outside the definition of "financial institutions" for the purposes of those statutes. The Justice Department asserts that the deterrent value of these statutes "is equally crucial for illicit activity in the digital assets space." Although banks and other financial institutions have long been subject to criminal penalties for notifying the subject of a grand jury subpoena about the existence of the subpoena, this prohibition does not apply to MSBs, and this would be a significant change for crypto firms acting as MSBs.[7][6]
>
> ***2. Strengthening the law criminalizing the operation of unlicensed MSBs***. The DOJ recommends amendments to or the issuance of regulations under 18 U.S.C. § 1960 to clarify that the statute applies to VASPs "providing services that enable their users to transfer digital assets in a manner analogous to traditional money transmitting business." Currently, certain VASP models occupy an ambiguous place under federal statutes and regulations governing MSBs. While the DOJ Report does not elaborate on the specific types of VASP activities that the statute should capture, the Justice Department's proposal, on its face, appears to favor casting a wider net. The DOJ further recommends increasing the maximum penalty and expanding the maximum sentence (from five years to ten) for violations of 18 U.S.C. § 1960, and ratifying existing case law concerning the *mens rea* for a violation of the law.[8]
>
> ***3. Extending the statute of limitations of certain statutes to account for the complexities of digital assets investigations***. To address the fact that investigations involving digital assets "can be complex and lengthy in duration," the DOJ recommends that Congress extend the default federal statute of limitations from five years to ten years "for all crimes (or an enumerated set of offenses) that involve the transfer of digital assets."

In addition to the three priority items summarized above, the DOJ Report proposes a number of other regulatory and legislative changes. Notable examples include:

- ***Application of the BSA to NFT platforms.*** Noting that the "explosive growth" of the NFT market could give rise to "substantial money laundering concerns," the DOJ Report recommends amending the BSA and its implementing regulations to "make clear that its key AML/CFT provisions— including the obligations to have customer identification programs and report suspicious transactions to regulators—apply to NFT platforms, including online auction houses and digital art galleries."
- ***Stricter sentencing guidelines for BSA violations.*** The DOJ Report proposes amending federal Sentencing Guidelines for criminal BSA violations to better reflect "the gravity of BSA violations that facilitate money laundering

and other illicit activity." The DOJ Report recommends the implementation of stricter standards for such violations, which could include "the addition of specific offense characteristics tied to the nature of the BSA violation." The DOJ Report states that the Sentencing Guidelines should recognize that "organizations with weak or non-existent BSA policies and programs in the digital assets industry facilitate the illicit use of digital assets and allow criminals to cash out or otherwise profit from their crimes."

- ***Expanding civil and criminal forfeiture authorities to commodities-related violations and designating commodities violations as a "specified unlawful activity."*** The DOJ Report proposes designating commodities fraud as a "specified unlawful activity" (i.e., a predicate offense) for the purposes of 18 U.S.C. §§ 1956 and 1957, and in so doing providing civil and criminal forfeiture authorities for commodities-related violations.
- ***Application of the Travel Rule to virtual assets.*** The DOJ Report supports FinCEN's issuance of a final rule applying the Travel Rule to transactions above the applicable threshold involving convertible virtual currency, as well as transactions involving digital assets with legal tender status. [9]

Summary of Illicit Finance Action Plan

On March 1, 2022, the Treasury Department published the 2022 National Risk Assessments (NRAs) on Money Laundering, Terrorist Financing and Proliferation Financing, providing Treasury's analysis of the most significant illicit finance threats, vulnerabilities, and risks to the U.S. financial system. The Illicit Finance Action Plan sets forth actions to address the risks identified in the NRAs, specifically those related to digital assets.[10]

In large part, the NRAs aligned with previous publications in 2015 and 2018, but addressed changes to the illicit finance landscape that were the result of, among other things, the increased adoption of digital payment systems and financial services. Informed by the threats, risks, and vulnerabilities associated with digital assets described in the NRAs, as well as the four priorities identified in the Illicit Financing Strategy, the Illicit Finance Action Plan lists seven priority actions (with accompanying supporting actions) to which the U.S. government is committed. The action items break little new ground, and largely reflect the continuation of ongoing initiatives. This is essentially acknowledged by Treasury, as the Illicit Finance Action Plan states that most of the supporting actions "continue and deepen ongoing Treasury work"; however, some of the supporting actions include new efforts such as preparing an illicit finance risk assessment on DeFi. Below, we discuss in more detail the actions identified in the Treasury Department's Illicit Finance Action Plan.

Priority action 1 – Monitoring emerging risks

The Illicit Finance Action Plan states that the United States will continue to monitor the development of the digital assets industry, in addition to the industry's attendant financial crimes risks, to identify gaps in U.S. legal, regulatory, and supervisory regimes. The findings will inform further prioritization and resourcing of the other priority actions identified in the Action Plan. Supporting actions include:

1. Preparing and publishing a risk assessment by February 24, 2023 on the money laundering and terrorist financing risks related to DeFi;

2. Preparing and publishing a risk assessment by July 2023 on the money laundering and terrorist financing risks related to NFTs;

3. Leading efforts at the FATF to monitor the digital asset sector for material changes or developments that necessitate further revision or clarification of the FATF standards;

4. Monitoring the adoption of digital assets as legal tender and central bank digital currencies (CBDCs) in other jurisdictions, analyzing the illicit finance risks associated with CBDCs, and engaging with countries to ensure appropriate AML controls are in place; and

5. Supporting the Federal Reserve's CBDC research and technical experimentation efforts.

Priority action 2 – Improving global AML regulation and enforcement

The Illicit Finance Action Plan states that addressing weaknesses in AML regulation, supervision, and enforcement in foreign jurisdictions is a priority for the U.S. government. To support this work, the U.S. government will continue to work through the FATF to promote the effective implementation of measures related to digital assets. Supporting actions include:

1. Partnering with G7 countries to urge foreign jurisdictions to implement the FATF standards for virtual assets and VASPs;

2. Engaging bilaterally with countries that the U.S. government assesses will be receptive to engagement and have high illicit financing risks related to virtual assets to encourage and support implementation of the FATF standards for virtual assets and VASPs;

3. Working with Congress to secure funding requested in the 2023 Budget to support efforts to support the implementation of the FATF standards for virtual assets and VASPs abroad; and

4. Sharing information with partner nations, as appropriate, to support international investigations and prosecutions on the abuse of digital assets.

Priority action 3 – Updating Bank Secrecy Act regulations

To address the illicit financing risks identified in Priority Action 1, the Treasury Department will continue to evaluate whether the U.S. AML regulatory regime can continue to safeguard the U.S. financial system from illicit financial activity, whether facilitated by fiat currency or digital assets. Supporting actions include:

1. Continuing to review comments received in response to ongoing digital asset?related Notices of Proposed Rulemakings and address them, as appropriate, in any rules; and[11]

2. Evaluating the emergence and evolution of digital assets to determine whether any gaps exist in the current AML/CFT framework or its application. Notably, this could include the continued consideration within the U.S. government of the utility and risks of lowering the Travel Rule's $3,000 threshold.

Priority action 4 – Strengthening U.S. AML supervision of virtual asset activities

The Illicit Finance Action Plan notes that the Treasury Department will continue to engage with intergovernmental standard?setting bodies such as the FATF to ensure that digital asset supervision evolves in a uniform manner. The Treasury Department is working to ensure that VASPs doing business wholly or in substantial part in the United States, wherever located, register with the requisite regulatory bodies at the state or federal level, and that they comply with applicable BSA obligations. Supporting actions include:

1. Strengthening FinCEN's existing supervisory enforcement function, particularly through examinations and related compliance and enforcement investigations and actions;

2. Pursuing enforcement activity, as appropriate;

3. Coordinating with state supervisors responsible for VASPs to promote standardization and coordination of state licensing and AML/CFT obligations, as well as supervision for MSBs, and improving state?state and state?federal coordination more broadly; and

4. Producing guidance, alerts, and notices on concerning illicit finance trends and developments in the digital asset space to encourage the filing of suspicious activity reports related to such activity.

Priority action 5 – Holding cybercriminals and other illicit actors accountable

The Illicit Finance Strategy reinforces the U.S. government's commitment to exposing and disrupting illicit actors and addressing the abuse of digital assets. Actions to disrupt such illicit activities will include seizures, criminal prosecutions, civil enforcement, and targeted sanctions designations. Mixing services, darknet markets, and non?compliant VASPs used to launder or cash out illicit funds into fiat currency are of primary concern. Supporting actions include:

1. Investigating, detecting, disrupting, and prosecuting the illicit use of digital assets, including for money laundering, ransomware, terrorist financing, fraud, theft, digital extortion, and sanctions evasion; and

2. Placing digital asset wallets and addresses associated with illicit use of digital assets on the List of Specially Designated Nationals and Blocked Persons to support industry screening for and blocking or rejecting transactions associated with blocked persons.

Priority action 6 – Engaging with the private sector

According to the Illicit Finance Action Plan, the U.S. government will continue to engage with private industry to ensure that U.S. entities understand existing AML obligations and illicit finance risks associated with digital assets. Supporting actions include:

1. Expanding FinCEN's 314(a) program to include more VASPs;[12]

2. Encouraging VASPs to participate in and use 314(b) voluntary information?sharing mechanisms to enhance the collection and reporting of potentially suspicious transactions that involve digital assets; and[13]

3. Enabling financial institutions to improve their ability to identify threats and vulnerabilities associated with criminal activity in the virtual asset space through further information sharing on cyber vulnerabilities and illicit financing risks.

Priority action 7 – Supporting U.S. leadership in financial and payments technology

The Illicit Finance Action Plan also acknowledges the evolution of the U.S. domestic payments system, including real?time payment solutions and digital channels such as same?day automated?clearing house transactions and permissioned blockchain-based payment systems. The U.S. government is committed to supporting the pace of innovation while also combatting emerging illicit finance risks. Supporting Actions include:

1. Considering ways to modernize the U.S. payments infrastructure;

2. Working with interagency partners and Congress to implement recommendations stemming from the President's Working Group on Financial Markets on Stablecoins; and

3. Supporting U.S. companies' collective pursuit of developing new financial technologies through regulatory and supervisory guidance, symposia, tech sprints, and FinCEN Innovation Hours.

Summary of request for comment

On September 19, 2022, the Treasury Department issued an RFC to collect feedback on the Treasury Department's ongoing efforts to assess and mitigate the illicit finance risks associated with digital assets. Commenters are encouraged to address the questions in the RFC, or, in the alternative, to provide any other relevant comments. The RFC provides a list of 23 questions, which address issues including the following:

- **Illicit finance risks.** The Treasury Department seeks comments on whether it has comprehensively defined the illicit financing risks associated with digital assets and how future technological innovations in digital assets may present new illicit finance risks (or mitigate illicit finance risks).
- **AML regulation and supervision.** The Treasury Department seeks comments on additional steps the U.S. government should take to more effectively deter, detect, and disrupt the misuse of digital assets and digital asset service providers by criminals. Comments can include critiques of existing regulatory obligations and suggestions for more suitable regulatory changes.
- **Global implementation of AML standards.** The Treasury Department seeks feedback on how it can most effectively support consistent implementation of global AML standards across jurisdictions, including the identification of specific countries or jurisdictions where the U.S. government should focus its efforts.
- **Private sector engagement.** The Treasury Department seeks comments on ways in which the agency can better engage with the private sector, 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.
- **Central bank digital currencies.** The Treasury Department seeks comments on how it can most effectively support the incorporation of AML controls into a potential U.S. CBDC design.

As noted above, comments are due by November 3, 2022. As both regulators and financial institutions adapt to the evolving landscape of financial crime, FinCEN encourages stakeholders to make their voices heard.

Looking forward

As can be said of Executive Order 14067 itself, the DOJ Report and the Treasury's Action Plan reflect the fact that the digital assets sector has increasingly shifted from an area of interest for regulators to one of primary concern. Likewise, the substance of the DOJ Report and the Illicit Finance Action Plan reflects the proactive posture that both the Justice and Treasury Departments have taken towards the enforcement and implementation of AML standards in the digital assets ecosystem. In the near term, however, it is unclear whether and to what extent the legislative and policy recommendations of the DOJ and Treasury will be translated into law. The current divided state of Congress, the approaching midterm elections, and otherwise shifting congressional priorities are likely to delay further substantive revisions to the BSA in the immediate future. Likewise, as FinCEN is currently overburdened with other congressionally mandated rulemakings and facing significant resource and funding challenges, it is questionable whether the agency has the capacity to undertake additional rulemakings. Nevertheless, to the extent that the DOJ Report and the Illicit Finance Action Plan signal a concrete regulatory focus on the digital assets ecosystem, they can reasonably be seen to reflect the shape of things to come.

Exec. Order. No. 14,067 (2022), available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/.[1]

We discuss the Treasury Department's the National Strategy for Combatting Terrorist and Other Illicit Financing Risks in this May 9, 2022 client update.[2]

Department of Justice, The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets (Sep. 2022), https://www.justice.gov/ag/page/file/1535236/download.[3]

The DOJ's discussion of the illicit uses of digital assets—and the specific typologies of behavior that the DOJ identifies—largely overlap with those described in recently released guidance regarding digital assets, including the Treasury Department's 2022 National Money Laundering Risk Assessment, in addition to the Financial Action Task Force's (the "FATF") Updated Guidance on Virtual Assets and Virtual Assets Service Providers. For a discussion of FATF's guidance and the risk typologies discussed, see Davis Polk's November 1, 2021 client update, available at: https://www.davispolk.com/insights/client-update/financial-action-task-force-issues-updated-guidance-virtual-assets.[4]

Department of Justice, Press Release, Justice Department Announces Report on Digital Assets and Launches Nationwide Network (Sep. 16, 2022), https://www.justice.gov/opa/pr/justice-department-announces-report-digital-assets-and-launches-nationwide-network.[5]

31 U.S.C. § 5312(a)(2).[6]

See 12 U.S.C. § 3420(b); 18 U.S.C. § 1510(b).[7]

18 U.S.C. § 1960 prohibits unlicensed money transmitting businesses.[8]

Board of Governors of the Federal Reserve System, FinCEN, "Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement To Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets With Legal Tender Status," 85 Fed. Reg. 68,005 (Oct. 27, 2020).[9]

We elaborate on the specific risks identified in the NRAs in Davis Polk's March 9, 2022 client update.[10]

The Illicit Finance Action Plan specifically highlights the "Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement to Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets with Legal Tender Status" and "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" proposed rulemakings.[11]

31 CFR Part 1010.520; Section 314(a) of the USA PATRIOT Act gives the Treasury Department the authority to contact financial institutions to locate accounts and transactions of persons identified by law enforcement that may be involved in terrorism or money laundering. FinCEN'S 314(a) Fact Sheet provides additional guidance. https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf.[12]

USA PATRIOT Act Section 314(b) provides a safe harbor from civil liability to financial institutions which, upon providing notice to the Treasury Department, share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist financing activity.[13]

Resources
Crypto Regulation Hub

Visit our Crypto Regulation Hub for links to congressional proposals related to the regulation of crypto assets and other helpful materials.

Explore our crypto resources

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres
+1 212 450 4724
greg.andres@davispolk.com

Kendall Howell
+1 202 962 7068
kendall.howell@davispolk.com

Paul Marquardt
+1 202 962 7156
paul.marquardt@davispolk.com

Tatiana R. Martins
+1 212 450 4085
tatiana.martins@davispolk.com

John B. Reynolds III
+1 202 962 7143
john.reynolds@davispolk.com

Will Schisa
+1 202 962 7129
will.schisa@davispolk.com

Daniel P. Stipano
+1 202 962 7012
dan.stipano@davispolk.com

Charles Marshall Wilson
+1 202 962 7130
charles.wilson@davispolk.com