WINSTON & STRAWN LLP

DIGITAL ASSETS & BLOCKCHAIN TECHNOLOGY GROUP

The Future of Digital Assets Regulation in the United States

TREASURY AND DOJ SIGNAL TOUGH REGULATION AND STRICT ENFORCEMENT

On September 16, 2022, the U.S. Department of the Treasury ("Treasury"), the Department of Justice (the "DOJ"), and other U.S. government agencies released eight highly anticipated reports[1] (the "Reports") on different aspects of digital asset regulation, setting forth the agencies' respective legislative, regulatory, and policy recommendations and priorities. The Reports were issued in response to White House Executive Order 14067 on Ensuring Responsible Development of Digital Assets (the "Executive Order"), which calls for a whole-of-government alignment of the federal government's approach to digital assets.

The Reports confirm the Biden-Harris Administration's acknowledgement that digital assets have potential benefits and are likely to remain a component of the U.S. financial system, but that the proliferation of the asset class presents unique risks that should be addressed. While the Reports provide some insight into the Administration's thinking about digital assets and articulate some recommendations and "calls to action," many significant regulatory questions remain unaddressed.

This Winston Alert highlights the most significant aspects of the Reports, including:

- **Regulatory and procedural reform**: The Reports call for coordination among federal agencies to increase regulation of digital assets, pursue investigations of misuse, issue plain-English reports to increase digital asset literacy, and amend anti-money laundering ("AML") and money transfer laws to apply to digital assets.

- **Illicit activity, money-laundering, and terrorism financing risks**: The Reports emphasize the risks posed by digital assets for domestic and international AML programs and efforts to counter terrorism financing. The pseudonymity, irreversibility of transactions, and current information asymmetry between issuers of digital assets and consumers and investors create an environment conducive to illicit activity that may harm U.S. consumers, businesses, and investors.

- **Populations vulnerable to disparate impacts of digital assets**: The Reports discuss the delicate balance between the potential benefits of digital assets for unbanked and underbanked populations and the risks they pose for these groups. While these groups stand to benefit from new technologies, they may also be disparately vulnerable to their misuses.

- **Populations vulnerable to disparate impacts of digital assets**: The Reports discuss the delicate balance between the potential benefits of digital assets for unbanked and underbanked populations and the risks they pose for these groups. While these groups stand to benefit from new technologies, they may also be disparately vulnerable to their misuses.

- **U.S. central bank digital currency exploration**: Treasury recommends further study of the risks and benefits of a central bank digital currency in the United States, while also suggesting that one is not imminent in the United States and may be determined not in the best interest of the American people.

ACTION PLAN TO ADDRESS ILLICIT FINANCING RISKS OF DIGITAL ASSETS (U.S. DEPARTMENT OF THE TREASURY)

Treasury published its "Action Plan to Address Illicit Financing Risks of Digital Assets" ("Action Plan") as mandated by Section 7(c) of the Executive Order, which directed the development of a coordinated interagency action plan for "mitigating the digital asset-related illicit finance and national security risks addressed in the updated strategy." In the Action Plan, Treasury identifies several aspects of digital assets that are of concern for Treasury, including the use of digital assets in money laundering, ransomware crimes, revenue generation and sanctions evasions by states and groups, and financing of terrorist organizations. As a result, Treasury presented seven "priority actions" and supporting actions to address these issues.

FEATURES OF DIGITAL ASSETS

Treasury identified several features of digital assets and digital asset businesses that pose risks to proper financial security and oversight, including:

- Gaps in AML regimes across countries;

- Anonymous features of digital assets;

- Disintermediation of virtual assets, actual or otherwise; and

- Virtual asset service providers ("VASPs") that are non-compliant with AML and other regulatory obligations.

Treasury focused on the obligations of VASPs and peer-to-peer ("P2P") service providers who engage in the business of transacting digital assets through "unhosted" digital wallets—*i.e.*, wallets not held by any financial institution or VASP. Treasury stated that VASPs and P2P service providers can be subject to U.S. AML obligations if they operate wholly or in substantial part in the United States, regardless of where they are located. Such businesses and individuals could be required to register with the Financial Crimes Enforcement Network ("FinCEN") as money services businesses, implement an effective AML program, or abide by recordkeeping and reporting obligations such as the requirement to file Suspicious Activity Reports ("SARs"). Treasury also warned that P2P service providers and decentralized finance ("DeFi") services that purport to transact through unhosted wallets may nonetheless be subject to AML and countering-the-financing-of-terrorism ("CFT") obligations as money transmitters when they transfer currency, funds, or assets of value.

PRIORITY AND SUPPORTING ACTIONS

Treasury introduced seven priority actions to mitigate the perceived threats and risks of digital assets. In most of the supporting actions to these priorities, Treasury identified itself as the lead department to pursue the objectives, while also recognizing the importance of interagency coordination. The priority actions listed in the Action Plan are:

- Monitoring emerging risks through collection of information and investing in technology and training;
- Improving global AML regulation and enforcement;
- Updating Bank Secrecy Act ("BSA") regulations to address illicit financing risks;
- Strengthening U.S. AML supervision of virtual asset activities and promoting standardization of AML/CFT obligations across states;
- Holding accountable cybercriminals and other illicit actors through seizures, criminal prosecutions, civil enforcement, and targeted sanctions designations;
- Engaging with the private sector and exchanging information on illicit financing risks and AML obligations; and
- Supporting U.S. leadership in financial and payments technology, such as real-time payment solutions and stablecoins.

While most of the supporting actions were continuations of Treasury's previous work, some of the supporting actions were new. For example, Treasury intends to publish an illicit finance risk assessment on DeFi and its role in money laundering and terrorist financing risks by February 24, 2023. Treasury also plans to convene state supervisors to promote standardization and coordination of state licensing and AML obligations of VASPs. Furthermore, Treasury briefly noted the increasing global interest in Central Bank Digital Currencies ("CBDC"), which Treasury believes must be designed to comply with global AML standards. Treasury plans to monitor both domestic and foreign CBDC development initiatives and consider implications for AML/CFT controls.

CRYPTO-ASSETS: IMPLICATIONS FOR CONSUMERS, INVESTORS, AND BUSINESSES (U.S. DEPARTMENT OF THE TREASURY)

In the Executive Order, the Biden Administration acknowledges that continued expansion of crypto-based technology could have profound implications for the users of digital assets—namely, consumers, investors, and businesses. In this Report, Treasury reviews current digital asset markets and trends that inform the potential opportunities and risks associated with their use. Treasury also discusses the implications of these opportunities and risks for consumers, investors, and businesses, considering those aspects affecting populations vulnerable to disparate impacts and proposing a multi-prong recommendation to address these risks.

CRYPTO-ASSET MARKET TRENDS, USES, AND OPPORTUNITIES

As of August 20, 2022, the market capitalization of Bitcoin was approximately $404.8 billion. Moreover, there has been an exponential growth in the number of coins and tokens, with an estimated handful of crypto-assets in 2013, to more than 2,800 by the end of 2019, and to nearly 10,400 at the beginning of 2022. With this rapid growth, the number of digital asset trading platforms proliferated, significantly expanding the possibility for consumers, investors, and businesses to engage in an ever-changing variety of financial and non-financial activities.

- Treasury explains that, despite the rapid expansion of digital assets, the uses of these products can be classified into the following broad categories:
- Crypto asset-based alternatives to traditional financial products and services;
- Financial market and payment system infrastructure; and

- Potential cases for other consumer and commercial uses by individuals and businesses, for example, non-fungible tokens ("NFTs"), gaming, records, identity, and supply-chain management.

RISKS AND EXPOSURES FOR CONSUMERS, INVESTORS, BUSINESSES

Existing use cases of digital assets and their potential opportunities come with risks, which Treasury categorizes into three groups: (1) conduct risks, including product, investor, consumer, and business protection; (2) operational risks, including the technology-specific risks of crypto-assets and systems; and (3) risks arising from crypto-asset intermediation.

Some of the risks are unique to digital assets while others are simply a form of risk already present in traditional finance markets that are heightened due to the specific attributes of crypto-assets. The lack of transparency, the uncertain regulatory environment, and the fact that crypto-assets have relatively novel and rapidly developing applications can give rise to fraud, theft, scams, abusive market practices, disclosure gaps, criminal activity, and operational failures. The unique features of the crypto-asset ecosystem can also make it attractive for unlawful activity—ongoing development and evolution of the underlying technology, pseudonymity, irreversibility of transactions, and the current asymmetry of information between issuers of crypto-assets and consumers and investors foster an environment ripe for misuse.

Despite efforts from regulatory authorities, chiefly including the Federal Reserve, Federal Deposit Insurance Corporation (FDIC), DOJ, and Commodity Futures Trading Commission ("CFTC"), Treasury explains that consumers, investors, and businesses remain exposed to risk that either arises from bad actors or occurs as a result of the products and services not being in compliance with regulatory requirements, regardless of intent.

Treasury notes that risks arise from non-compliance with the following:

- Extensive non-disclosure requirements for registered exchanges, products, and intermediaries that are designed to provide investors and customers with material information; and

- The requirements around market conduct that are designed to provide fair, orderly, and efficient markets.

Treasury discusses the disparate impact of the aforementioned risks for more vulnerable populations, which include low-income individuals; communities that have been historically excluded from the financial system or subject to discrimination in accessing financial services or wealth-building opportunities; and unbanked and underbanked populations. While digital assets may present opportunities to expand access to financial services, some of these populations may be more exposed to the volatility and risks of crypto-asset investing; others may be at greater risk of being preyed upon by targeted marketing, fraud, and scams; and still others may be more limited in their capacity to recover from financial harm. Treasury cites a survey from the Federal Reserve Board finding 29% of respondents who held crypto-assets for investment purposes had an annual household income of less than $50,000, stressing the urgency in examining and responding to the potential disparate impacts of crypto-asset activities.

RECOMMENDATIONS

In view of the risks and opportunities associated with crypto-assets, Treasury sets forth certain actions to be taken in the interim while stakeholders continue to deliberate on legislative

proposals on the subject to protect U.S. consumers and businesses:

- **Recommendation 1 – Expand and Increase Investigations and Enforcement, and Cross-Agency Coordination:** U.S. regulatory and law enforcement agencies should vigilantly monitor the crypto-asset sector for unlawful activity, aggressively pursue investigations, and continue to bring civil and criminal actions to enforce applicable laws and protect consumers, investors, and the market. Treasury additionally calls for coordination of law-enforcement officials and regulators to combat fraud, deter unlawful behavior, and improve practices in crypto-asset markets, in addition to sharing information regarding fraudulent, misleading, or manipulative market practices they are observing and investigating to ensure broad and consistent enforcement and supplement private sector analytic tools.

- **Recommendation 2 – Provide Guidance:** U.S. regulatory agencies should continue using existing authorities to issue supervisory guidance and rules, as needed, to address emerging risks in crypto-asset products and services for consumers, investors, and businesses. Agencies should collaboratively promote consistent and comprehensive oversight of crypto-assets. Given significant interest of individual consumers, investors, and populations vulnerable to disparate impacts in crypto-assets, regulations should issue guidance, interpretations, and rulemaking related to crypto-assets in plain language.

- **Recommendation 3 – Access to Trustworthy Information:** U.S. authorities should work individually and through the Financial Literacy and Education Commission to ensure that U.S. consumers, investors, and businesses have access to consumer-friendly, consistent, and trustworthy information on crypto-assets. Such materials should highlight risks associated with use of crypto-assets; identify and warn against common practices employed by perpetrators of fraud, thefts, and scams; and provide information on how to report unlawful practices.

CLIMATE AND ENERGY IMPLICATIONS OF CRYPTO-ASSETS IN THE UNITED STATES (THE WHITE HOUSE)

In this Report, the White House recognizes that digital assets require a significant amount of energy resources and may have harmful effects on the environment. At the same time, digital assets play an important role in climate-monitoring and -mitigating initiatives, potentially lowering their harmful effects with further development. The Office of Science and Technology Policy ("OSTP") issued a Report addressing four questions posed by the Executive Order:

How do digital assets effect energy usage, including grid management and reliability, energy efficiency incentives and standards, and sources of energy supply?

The OSTP recognizes that digital assets may consume a significant amount of electricity, with crypto assets being a major culprit. For example, crypto assets in August 2022 used the equivalent of 0.4% to 0.9% of annual global electricity usage, comparable to the annual electricity usage of all non–crypto asset data centers in the world. As of August 2022, two blockchains in particular, Ethereum and Bitcoin, account for the vast majority of electricity usage—60% to 77% and 20% to 39%, respectively. In turn, crypto-asset operations and mining may fluctuate, impacting consumers and energy infrastructure. In New York, crypto-asset mining increased annual household electric bills by $82 and small-business electric bills by $164. Crypto assets also continuously use power, which can affect power grids and diminish equipment.

However, the OSTP recognizes that energy usage varies substantially with different crypto assets. Proof-of-work blockchains use significantly more energy than proof-of-stage mechanisms. Such findings may promote and incentivize crypto-asset leaders to innovate and develop more energy-efficient mechanisms.

What is the scale of climate, energy, and environmental impacts of digital assets relative to other energy uses, and what innovations and policies are needed in the underlying data to enable robust comparisons?

Overall, crypto-asset activity in the United States results in carbon dioxide emissions of about 25 to 50 million metric tons per year. Certain regions, such as the Great Plains, that rely predominantly on coal power may use more carbon-intensive energy sources than others. In addition, crypto assets have other environmental effects, such as air and water pollution, noise pollution, and electronic waste. However, the OSTP recognizes that there are ways to motivate zero-emission operations. This may include contracting or constructing new clean electricity to power mining or using existing renewable electricity.

What are the potential uses of blockchain technology that could support climate-monitoring or mitigating technologies?

The OSTP recognizes that blockchain technologies can play a powerful role in various energy management, monitoring, and regulation frameworks. Specifically, the OSTP highlights the use of distributed-ledger technologies ("DLT") and blockchain in these capacities. The OSTP states that DLT may play a role in enhancing environmental markets, although certain markets, such as highly centralized compliance markets, may not be as applicable. The OSTP does emphasize that DLT may play a more powerful role in organizing distributed-energy resources. For example, DLT could serve as a digital ledger for the registration, authentication, and participation of distributed-energy resources like electric vehicles, fuel cells, or solar-power systems. DLT could also decentralize and automate power infrastructures, such as an electricity grid, and increase security and reliability.

Ultimately, the use of blockchain technology and DLT may facilitate the development of new environmental and energy markets that could spur innovation. DLT could help create peer-to-peer energy microgrids that localize energy consumption and reduce system congestion.

What key policy decisions, critical innovations, research and development, and assessment tools are needed to minimize or mitigate the climate, energy, and environmental implications of digital assets?

Ultimately, the OSTP provides six actions for consideration:

- The OSTP recommends that federal agencies work collaboratively to minimize greenhouse gas ("GHG") emissions, environmental justice impacts, and other local impacts from crypto assets. This may include creating new energy standards, including low water usage, low noise generation, or clean-energy usage. The OSTP also recommends the use of potential congressional legislation or executive actions to reduce impacts.

- The OSTP recommends ensuring energy reliability. This includes actions by the Department of Energy and various regional entities conducting reliability assessments of crypto-asset mining operations, and potentially developing reliability standards.

- The OSTP recommends obtaining data to understand, monitor, and mitigate impacts. This includes collaboration with federal agencies

to collect and analyze more-accurate data—such as mining-energy usage, power purchase agreements, and other mandatory-response participation—to make decisions on implications of crypto assets.

- The OSTP recommends federal agencies and regulations to promulgate and regularly update energy conservation standards for crypto-asset operations.

- The OSTP recommends that the crypto-asset industry work with further transparency. This includes publicly reporting crypto-asset mining locations, annual electricity usage, GHG emissions, and electronic-waste-recycling performance.

- The OSTP recommends further research to improve understanding and innovation. This includes using federal agencies to promote and support research that improves the sustainability of digital assets. Additionally, further research and development priorities could emphasize innovation in digital-asset technologies, such as reducing environmental impacts and improving efficiencies.

U.S. CENTRAL BANK DIGITAL CURRENCY: POLICY OBJECTIVES & TECHNICAL EVALUATIONS (THE WHITE HOUSE)

In the Executive Order, the Biden-Harris Administration stresses the need for research and development concerning the potential design and deployment options of a U.S. CBDC. These Reports issued by the White House discuss the policy objectives outlined in the Executive Order and analyze technical design choices for a U.S. CBDC and how such choices would impact the policy objectives for a U.S. CBDC.

A CBDC is a digital form of a country's sovereign currency. The White House states that this novel type of central bank money may provide a range of benefits for American consumers, investors, and businesses. However, a U.S. CBDC also poses potential risks, ranging from the stability of the financial system to the protection of sensitive data.

POLICY OBJECTIVES FOR A U.S. CBDC SYSTEM

Building on the policy objectives described in the Executive Order, the White House asserts that a U.S. CBDC should support the following objectives:

- Provide benefits and mitigate risks for consumers, investors, and businesses;
- Promote economic growth and financial stability and mitigate systemic risk;
- Improve payment systems;
- Ensure the global financial system has transparency, connectivity, and platform and architecture interoperability or transferability, as appropriate;
- Advance financial inclusion and equity;
- Protect national security;
- Provide ability to exercise human rights; and
- Align with democratic and environmental values, including privacy protections

TECHNICAL DESIGN CHOICES FOR A U.S. CBDC SYSTEM

In deciding whether a CBDC is in the best interest of the United States, policymakers are urged to carefully consider the design choices for the CBDC system under consideration. The White House focuses on 18 design choices, divided into six categories: participants, governance, security, transactions, data, and adjustment. In discussing the different design options, the White House assists policymakers in understanding the technical design choices and their associated tradeoffs, keeping the policy objectives top of mind. The White House

clearly discloses that, through its discussion of design choices, it is not presupposing that a CBDC system would use any particular technology, and it does not take any position on whether establishing a CBDC system would be in the best interest of the United States.

FEASIBILITY AND RESOURCES FOR A U.S. CBDC SYSTEM MINIMUM VIABLE PRODUCT

In the event the United States decides that launching a CBDC system is in the best interest of the United States, the White House provides an outline for steps that could be taken to pursue the effort to deploy a CBDC minimum viable product ("CBDC MVP"). It is not likely that a presupposed design for a CBDC system can succeed without testing. The development of a CBDC MVP would aim to validate the assumptions, understandings, and implication of introducing this novel financial instrument and technological product into the market.

Many other jurisdictions are conducting research and development related to CBDC systems, such as establishing research or pilots, or even deploying early-state CBDCs. Approximately 90% of central banks are engaging in some work related to CBDCs and approximately 62% of central banks are conducting experiments or developing proofs-of-concept. Private-sector experimentation in the digital assets ecosystem has been much broader than experimentation related only to a CBDC system. Technological features that have been developed in the digital-asset ecosystem could be relevant to developing a U.S. CBDC system and should be examined for their ability to advance policy objectives for a U.S. CBDC system.

IMPACT OF A U.S. CBDC SYSTEM ON FEDERAL PROCESSES

The White House discusses the U.S. government work and services that would be affected by the inclusion of a U.S. CBDC system. If the U.S. government adopts a CBDC system, it is probable that CBDC would also be incorporated as an additional method to make or receive payments in a variety of situations. For example, the IRS might offer CBDC as an option for individuals, businesses, and organizations to pay their taxes and receive refunds. The White House points out that, despite the fact that since 1999 most U.S. government payments may be made electronically, there may be some cases in which CBDC could provide a unique benefit—such as cases where a one-time benefits payment needs to be made quickly or where traditional banking infrastructure is unavailable.

The technical challenge of incorporating CBDC payments would depend, in part, on the design choices of the CBDC system, the technical infrastructure at agencies, and the availability of talent to incorporate the CBDC system into agencies' infrastructure. Adoption of a U.S. CBDC system may introduce risks for U.S. government cybersecurity and privacy risks related to the collection, storage, and transmission of payment information associated with business-identifiable and personally identifiable information. The White House raises concern that attacks on the CBDC system could be used to compromise various aspects of agencies' infrastructure. Similarly, attacks on agencies' infrastructure could also be used to compromise parts of the CBDC system.

The Federal government's adoption and use of a CBDC system poses benefits and risks to customer experience. The White House highlights that it is the policy of the United States to prioritize improvements to service delivery and customer experience by reducing administrative hurdles, enhancing transparency, creating greater efficiencies across the Federal government, and redesigning compliance-oriented processes to improve customer experience and more directly meet the needs of the people of the United States. The adoption and use of a CBDC system poses

both benefits and risks to customer experience. While a CBDC may improve services such as prompt payment, and tracking and servicing of loans, it may also present obstacles for ideal customer experience or raise concerns about accessibility.

Whether the CBDC system fulfills the policy objective of equity and inclusion will depend on how it interacts with safety-net programs such as Medicare, Medicaid, Social Security, Supplemental Nutrition Assistance Program benefits, and unemployment insurance. The recipients of these programs are more likely to be lower-income, underbanked, and have limited access to fast broadband Internet.

RECOMMENDATIONS ON PREPARING FOR A U.S. CBDC SYSTEM

Additionally, the White House sets forth the following recommendations on preparing for a U.S. CBDC system:

- Advance Technical Work Related to Digital Assets: The White House recommends coordinating federal activities and research and development related to several technologies underpinning digital assets.

- Continue Digital Assets Research and Experimentation Within the Federal Reserve: The Federal Reserve is already doing significant experimentation on CBDC systems. The White House calls for other departments and agencies to pursue their own experimentation to tackle discrete questions involving the potential application of CBDC systems in their areas of responsibility.

- Establish a Research and Development Agenda: There are a significant number of open questions related to digital assets, including CBDC systems. This Report stresses the importance that the U.S. government highlight these open questions and direct resources and the research community towards solving them.

- Scale-Up Tech Capacity Across the Federal Government: The Federal government should have the technological infrastructure capacity and expertise needed to harness benefits and mitigate risks from digital assets. Should a CBDC be deemed in the national interest and pursued, federal departments and agencies will also need to realign their processes and capabilities, including but not limited to, facilitating CBDC payments to and from the public sector. Additionally, departments and agencies should continue taking general steps towards improving their information technology systems so they are well-maintained if steps are required to be taken to incorporate a CBDC system.

THE ROLE OF LAW ENFORCEMENT IN DIRECTING, INVESTIGATING, AND PROSECUTING CRIMINAL ACTIVITY RELATED TO DIGITAL ASSETS (THE DEPARTMENT OF JUSTICE)

On September 6, 2022, United States Attorney General Merrick Garland announced the release of a report on the Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets. This Report, which was issued pursuant to Section 5(b)(iii) of the Executive Order, was a collaborative effort prepared by the DOJ's National Cryptocurrency Enforcement Team ("NCET") in consultation with the Secretary of Treasury, the Secretary of Homeland Security, and multiple federal regulatory agencies that are expected to continue to play pivotal roles as part of a whole-of-government approach to regulating and ensuring the lawful use of digital assets.

In this Report, the DOJ addresses the different criminal exploitation typologies of digital assets, including (i) the use of cryptocurrency as a means of payment for or manner of facilitating criminal activity; (ii) the use of digital assets as a means of concealing illicit financial activity; and (iii) crimes involving or undermining the digital asset ecosystem. It notes the challenges raised by the growth of DeFi and NFTs and highlights examples of law-enforcement efforts to date, notwithstanding those challenges included in high-profile matters involving the Hydra darknet marketplace, the Bitfinex virtual currency exchange, and a first-of-its kind insider-trading case involving cryptocurrency recently brought by the United States Attorney's Office for the Southern District of New York. In this Report, the DOJ summarizes its various initiatives and the initiatives of other law-enforcement agencies, including the recently announced launch of the nationwide Digital Asset Coordinator ("DAC") Network by the DOJ's criminal division. Comprising of over 150 designated federal prosecutors from United States Attorney's Offices and different litigating components across the DOJ (including in the Criminal and National Security Divisions and law enforcement agencies such as the Federal Bureau of Investigation (FBI) and Drug Enforcement Administration (DEA), the network will serve as a forum for prosecutors to obtain and disseminate training, technical expertise, and guidance about the investigation and prosecution of digital asset crimes, with each DAC acting as its district's or litigating component's subject-matter expert on digital assets, serving as a first-line source of information and guidance about legal and technical matters related to these technologies. Led by the NCET working in close coordination with the DOJ criminal division's Computer Crime and Intellectual Property Section (CCIPS) and the Money Laundering and Asset Recovery (MLAR) Section digital currency initiatives, the network will also continue to raise awareness about the benefits of leveraging collaborative international and cross-border relationships in combating illicit activities related to digital assets.

This Report concludes with the following nine recommendations for improving law enforcement's ability to combat crypto-related crimes:

- **Expand the Anti-Tip-Off Provision:** The DOJ recommends that the existing Anti-Tip-Off provision (18 U.S.C. § 1510(b)), which makes it illegal for officers or agents of financial institutions to notify customers when their records are subpoenaed as part of a government investigation, be expanded to apply to VASPs operating as Money Service Businesses (MSBs) and cover crypto-related offenses.

- **Increase Penalties for Operating an Unlicensed Money Transmitting Business:** The DOJ proposes increasing the maximum sentence contained in 18 U.S.C. § 1960 for covered money transmitters that fail to register with FinCEN, fail to obtain the requisite state licensing, or otherwise transmit funds known to be criminally derived, from five to 10 years. It also suggests adding an "enhanced penalties provision" doubling or even tripling criminal fines (depending on whether the defendant is an individual or corporation) in instances involving a money transmitter's business of more than $1 million in a 12-month period. The DOJ additionally recommends codifying existing case law holding that the general-intent requirement included in the state-licensing prong of § 1960 apply to the federal-registration prong.

- **Extend Limitations Periods for Crypto-Related Crimes:** The DOJ recommends amending 18 U.S.C. § 3293 (which extends the mail and wire fraud statute of limitations to 10 years for offenses "affecting a financial institution") to provide for a 10-year statute of limitations for all crimes involving the transfer of digital assets, and amend § 3292 to provide for a longer tolling or "suspension" period in instances where the U.S. government seeks to obtain foreign evidence related to an offense involving the transfer of digital assets.

- **Expand Forfeiture Authority:** The DOJ proposes expanding criminal and civil forfeiture authority for commodities-related violations of the securities and commodities fraud statute (18 U.S.C. § 1348) and the Commodity Exchange Act (7 U.S.C. § 13(a)(2)).

- **Lift Monetary Limit on Administrative Forfeiture of Cryptocurrency:** The DOJ recommends that the $500,000 cap on administrative forfeiture be lifted, either via Treasury providing that cryptocurrency is not a monetary instrument subject to the cap or Congress amending 19 U.S.C. § 1607 to lift the cap with respect to cryptocurrency and other digital assets altogether.

- **Amend the Sentencing Guidelines for BSA Violations:** The DOJ suggests that the Sentencing Commission should amend U.S.S.G. § 2S1.3 (which covers structuring, failure to report transactions, filing false reports, etc.) to include the specific offense characteristics tied to BSA violations and/or tie the base offense level to the amount of funds involved in a BSA violation.

- **Apply the BSA's Recordkeeping/Travel Rule to Virtual Currency:** The DOJ proposes supporting FinCEN in its enforcement and implementation of a rule, once finalized, clarifying that the BSA's recordkeeping and travel rule regulations apply to transactions involving convertible virtual currency and digital assets with legal tender status.

- **Amend the BSA to Apply to NFT Platforms:** The DOJ suggests that the BSA should be amended to clarify that its key AML provisions apply to NFT platforms, including online auction houses and digital art galleries.

- **Fund Law Enforcement Operations:** Lastly, the DOJ suggests that Congress should seek funding for resources necessary to support digital asset-related investigations and hire personnel essential to addressing emerging threats related to digital assets.

In sum, the Biden-Harris Administration continues to build on its prior statements and the statements of high-level officials within the DOJ about the need for various departments and agencies across the government to work collaboratively and in close coordination with each other to prevent and disrupt the criminal exploitation of digital assets. The recommendations contained in this Report are also in line with Winston's past forecasts that the government will seek both to expand existing laws and regulations to cover the digital assets space and to create new vehicles through which to identify, investigate, prosecute, and adequately punish, as well as deter, the illicit use of digital assets.

Although various federal agencies have taken steps towards the exploration, regulation, and oversight of digital assets, the Reports highlight and identify the analysis necessary for these agencies to achieve a more unified and comprehensive approach to regulation and oversight of digital assets in the United States. The Reports also illustrate that the Biden Administration will closely and carefully continue to monitor digital asset developments; assess potential risk to the financial system; address misuse of and implementation of illicit technology to evade U.S. laws and harm consumers, investors, and businesses; and evaluate the threats and risks to the U.S. economy and the ability of the United States to maintain a dominant position in global finance.

While the Reports acknowledge the benefits of digital assets and novel financial systems, Treasury, DOJ, and other agencies make it clear that it has not yet been determined whether these digital assets are in the best interest of the United States, and they urge the public to proceed with caution. Ultimately, these Reports represent a major step forward in U.S. digital-asset policies but leave numerous questions for digital-asset clients about applicable regulatory frameworks.

Authors

CAROL ALEXIS CHEN
PARTNER
Los Angeles
+1 (213) 615-1820
cachen@winston.com

JEREMY CHU
ASSOCIATE
New York
+1 (212) 294-6614
jchu@winston.com

CARL FORNARIS
CO-CHAIR, DIGITAL ASSETS & BLOCKCHAIN TECHNOLOGY GROUP
Miami
+1 (305) 910-0626
cfornaris@winston.com

DHRUVA R. KRISHNA
ASSOCIATE
Los Angeles
+1 (213) 615-1926
dkrishna@winston.com

PEYTON POSTON
ASSOCIATE
Charlotte
+1 (704) 350-7839
pposton@winston.com

KIMBERLY A. PRIOR
CO-CHAIR, DIGITAL ASSETS & BLOCKCHAIN TECHNOLOGY GROUP
Miami
+1 (305) 910-0788
kprior@winston.com

JANELLE E. RODRIGUEZ-MENA
ASSOCIATE
Miami
+1 (305) 910-0522
jrodriguezmena@winston.com

DANIEL T. STABILE
CO-CHAIR, DIGITAL ASSETS & BLOCKCHAIN TECHNOLOGY GROUP
Miami \\ New York
+1 (305) 910-0787
dstabile@winston.com

DIGITAL ASSETS & BLOCKCHAIN TECHNOLOGY GROUP

Winston's cross-practice Digital Assets & Blockchain Technology Group provides accurate and efficient advice that helps clients navigate existing and developing legal challenges surrounding blockchain technologies. Our team draws upon experience from lawyers in our corporate, securities, tax, litigation, regulatory, and intellectual property practices, as well as others, to advise clients from startups and DAOs to the largest financial services firms in the world.

1. The complete Reports mandated by President Biden's Executive Order and issued by Treasury, DOJ, and White House explored in this Winston Alert can be located at the following links:
   - Action Plan to Address Illicit Financial Risks of Digital Assets issued by Treasury
   - Crypto-Assets: Implications for Consumers, Investors and Businesses issued by Treasury
   - The Future of Money and Payments issued by Treasury
   - Climate and Energy Implications of Crypto-Assets in the United States issued by the White House
   - Policy Objectives for a U.S. Central Bank Digital Currency System issued by the White House
   - Technical Evaluation for a U.S. Central Bank Digital Currency System issued by the White House
   - The Role of Law Enforcement in Directing, Investigating, and Prosecuting Criminal Activity Related to Digital Assets issued by the DOJ
   - Responsible Advancement of US Competitiveness in Digital Assets issued by the U.S. Department of Commerce
2. On September 20, 2022, Treasury issued a notice inviting interested members of the public to comment on digital asset-related illicit finance and national security risks as well as an action plan to mitigate such risks. Comments must be received on or before November 3, 2022.
3. Exec. Order No. 14067, 87 Fed. Reg. 40,881 (July 8, 2022).
4. According to Treasury, virtual assets are a subset of digital assets that does not include central bank digital currencies ("CBDCs") or representations of other financial assets, such as digitalized representations of existing securities or deposits. See U.S. DEP'T TREASURY, Fact Sheet: Action Plan to Address Illicit Financing Risks of Digital Assets (Sept. 20, 2022), https://home.treasury.gov/system/files/136/Fact-Sheet-Action-Plan-to-Address-Illicit-Financing-Risks-of-Digital-Assets.pdf.
5. The Ethereum Merge was executed on September 15, 2022, which completed Ethereum's transition from a proof-of-work to a proof-of-stake consensus. The Ethereum Merge eliminated the need for energy-intensive mining and reduced energy consumption by approximately 99%.