ALSTON & BIRD

WWW.ALSTON.COM

Blockchain & Digital Assets ADVISORY ■

MARCH 21, 2022

Breaking Down Key Areas of Biden's Executive Order on Ensuring Responsible Development of Digital Assets

On March 9, 2022, President Biden issued his Executive Order on Ensuring Responsible Development of Digital Assets. The Executive Order (EO) establishes policy objectives related to digital assets and directs agencies and other Executive Branch members to take actions in developing a coordinated government approach to meet these policy objectives.

Data Privacy

Consumer protection, privacy, and data security are all core consumer protections that will be evaluated by the Secretary of the Treasury and Secretary of Labor in consultation with the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), and Consumer Financial Protection Bureau (CFPB). Specifically, FTC Chair Lina Khan and CFPB Director Rohit Chopra will consider if privacy or consumer protection measures within their jurisdictions may be used to protect users of digital assets and whether additional measures may be needed to balance the need for digital anonymity with avoiding consumer deception.

Following the EO, Chopra released a statement echoing the need to study the capacity for consumer harm within the CFPB's subject-matter review of digital assets. "The Consumer Financial Protection Bureau is committed to working to promote competition and innovation, while also reducing the risks that digital assets could pose to our safety and security. We must make sure Americans in all financial markets are protected against errors, theft, or fraud."

Cybersecurity

Cybersecurity directives run through various components of the EO, underscoring the Administration's growing concern with the security and stability of digital assets. The EO states that the Secretary of the Treasury must work with the Secretary of Labor and other relevant agencies to determine what measures are needed to protect consumers, investors, and businesses amid the increased use of digital assets. With increased use of digital assets and exchanges there may be increased risk of fraud and theft, privacy and data breaches, unfair and abusive acts or practices, and other cyber-incidents. The director of the Office of Science and Technology Policy and the chief technology officer of the United States are similarly ordered to produce a technical evaluation with the same concerns in mind, in consultation with Treasury and the Federal Reserve.

The EO also emphasizes the Biden Administration's concern for the potential illicit use of digital assets and the related financial and national security concerns, which include "money laundering, cybercrime, and ransomware." Against the backdrop of the proliferation of ransomware attacks and recently imposed sanctions due to Russia's invasion of Ukraine, the EO calls for coordinated action across all relevant U.S. government agencies to mitigate these cyber-risks, which the EO treats as "finance and national security risks," and directs the agencies to work with U.S. allies and partners to ensure a secure international response.

Payments/Financial Regulation

While the Executive Order makes clear that digital assets are not exclusively a matter for the federal banking and other financial regulators to tackle, there are clearly central roles for these agencies in implementing the EO. In particular, it highlights a number of key topics that fall within the ambit of these agencies. These include both broad Administration policy focus and direction on more specific action items in the form of studies.

Of the broader policy themes, the EO highlights a focus on consumer protection and expansion of access to underbanked consumers, including for consumers using digital assets for payments, or for investment, as well as privacy matters. The order sets a tone of fostering "responsible development" of payments and other financial innovation and maintaining international competitiveness within a rules-based framework, but also points to gaps in regulation and supervision, raising potential concerns about financial stability and systemic risk, while promoting a broad policy approach of "same business, same risks, same rules."

Among the more specific topics, the EO establishes the Biden Administration's policy of support for research and development for a U.S. central bank digital currency (CBDC), including what the Federal Reserve has already begun. The EO goes further, however, to require a broad interagency study of U.S. CBDC design to be completed within 180 days. The EO gives specific direction on seven topics to be addressed in the report, including, importantly, the roles of the private sector in CBDC and private-sector-administered digital assets.

Further, the EO directs an interagency study, including policy recommendations, to be completed within 180 days on the implications of digital assets and changes in financial market and payment infrastructures on consumers, investors, businesses, and "equitable economic growth." Finally, the EO directs the Treasury Secretary to convene the Financial Stability Oversight Council and to generate a report on financial stability, regulatory gaps, and policy recommendations within 210 days.

Securities and Exchange Commission

The Executive Order did not charge the SEC with the task of developing a framework for application of the federal securities laws to cryptocurrencies, generally. Rather, the SEC will, through the interagency process, participate in the preparation of a broader report addressing "the implications of developments and adoption of digital assets and changes in financial market and payment system infrastructures for United States consumers, investors, businesses, and for equitable economic growth." As part of this report, the several agencies participating in its preparation will devise policy recommendations, including any suggested regulatory and legislative actions, to "protect United States consumers, investors, and businesses, and support expanding access to safe and affordable financial services."

In addition, the EO urges the heads of several financial service regulators, including the SEC, to consider the extent to which those regulators' existing investor and market protection mandates might accommodate measures to address the risks particular to digital assets and, if not, whether additional measures may need to be employed. To that end,

within the last year, the SEC's Division of Examinations issued a Risk Alert to covered investment advisers, broker-dealers, and transfer agents regarding the division's continued focus on digital asset securities and the Division of Enforcement brought a number of enforcement actions in the crypto space.

Anti-Money Laundering, Counter-Terrorist Financing, Know Your Customer, and Sanctions Compliance

In the Executive Order, the Administration seems to acknowledge that digital assets will continue to be used and adopted by the mainstream, and that as a by-product of their growth, illicit use of such technology will also grow. This mandate has elevated the government's regulatory interests over digital assets from merely consumer protection to the national security level. The EO requires the Secretary of the Treasury, in consultation with various other components of the federal government, to provide a supplement to its National Strategy for Combating Terrorist and Other Illicit Financing addressing how digital assets, such as cryptocurrencies, stablecoins, and CBDCs, pose illicit finance and sanctions risks and how these assets are being used by illicit actors.

The EO also requires the Treasury Secretary, in consultation with relevant agencies, to develop a coordinated action plan to mitigate the digital-asset-related illicit finance and national security risk identified in the supplement to the strategy. The plan must address the role of law enforcement and measures to increase financial services providers' compliance with anti-money laundering (AML) / counter-terrorist financing (CFT) obligations related to digital asset activities.

Above all, the Administration recognizes that the current set of rules may be insufficient to mitigate these risks to digital assets. Based on the EO's language articulating the urgency in regulating this fast-growing space, additional rulemaking is inevitable and may impact the following areas:

- New rules may require new types of entities to comply with AML / know your customer (KYC) obligations. Examples may be U.S.-based non-financial institutions that create or operate protocols in the decentralized finance sector and digital art/nonfungible token dealers that accept digital currencies as payment in exchange for the digital goods.
- Tighter requirements on AML/KYC/CTF/sanctions compliance by adjusting the elements of the risk-based approach to compliance, including the use of blockchain analytical tools and competence to do effective AML/CTF/sanctions risk assessment and review and specific guidance on filing of suspicious activity reports.

Concerns whether the existing regulatory regime is sufficient for sanctions risks have been heightened in recent weeks amid fears that Russia and Belarus, both known to have extensive involvement in the utilization of digital assets for both legitimate and illicit purposes, may use digital asset transfers as a means of blunting the impact of financial sector sanctions imposed by the United States and its allies. While media reports have arguably overblown the potential that digital asset transfers could be utilized at a sufficiently large scale to achieve such an outcome, it is certainly the case that digital assets have been one means by which individuals, entities, and foreign governments subject to U.S. sanctions have circumvented such sanctions.

Given these concerns, it is likely that the Department of the Treasury's Office of Foreign Assets Control, the agency with primary authority to implement U.S. sanctions, may take action on digital assets sooner than other federal agencies in light of concerns about Russian and Belarusian circumvention of sanctions.

Clients in the digital assets space should closely follow the proposed rules and guidelines that will be issued in the next six months to a year and be ready to make modifications to their existing AML/KYC/CTF programs to comply with the new digital economy.

Technology

The Executive Order sets forth as a principal policy objective ensuring digital asset technologies are "developed, designed, and implemented in a responsible manner that includes privacy and security in their architecture [and] integrates features and controls that defend against illicit exploitation." The EO does not discuss the steps the government will take to accomplish this, other than in relation to the technology used to implement a CBDC. The EO instructs the Office of Science and Technology Policy to submit within 180 days of the EO a technical evaluation of the infrastructure, capacity, and expertise needed to introduce a CBDC. Importantly, the evaluation will address technical risks of current and emerging and future technologies (e.g., quantum computing). The EO also directs that the evaluation consider the impact of a CBDC on the delivery of services by the government.

In January 2022, the Federal Reserve published "Money and Payments: The U.S. Dollar in the Age of Digital Transformation," explaining that the agency is exploring a wide range of design options, but a CBDC would need to be privacy-protected, intermediated, widely transferable, and identity-verified. Given the EO's explicit concerns and the Federal Reserve's signaling, a permissions-based distributed ledger technology (DLT) may be the technology most likely proposed by the evaluation so that the U.S. government could retain control over the supply, access, and administration of a CBDC. This evaluation could begin to narrow the options for approved technology platforms used for digital assets.

Environmental

Consistent with President Biden's whole-of-government approach to addressing threats posed by climate change, the Executive Order directs key federal agencies and offices to evaluate the effects DLT could have on the President's climate agenda. Within 180 days, the director of the Office of Science and Technology Policy, in consultation with the Secretary of the Treasury, Secretary of Energy, administrator of the Environmental Protection Agency, chair of the Council of Economic Advisers, assistant to the President and national climate advisor, and the heads of other relevant agencies, must submit a coordinated report to the President that addresses three areas of potential impacts.

First, the report must address the environmental impact, including energy usage, of the cryptocurrencies themselves by evaluating the mechanisms that are currently used to operate cryptocurrencies and alternatives to those mechanisms that could be used in the future. Second, the report must address the impact of cryptocurrencies on the ability of other entities to transition to a low- or no-carbon footprint. The EO specifically identifies the possible use of blockchain to support "monitoring or mitigating technologies to climate impacts, such as exchanging of liabilities for greenhouse gas emissions, water, and other natural or environmental assets." Third, the report must cover any impacts of digital currencies on energy policy, including the reliability and management of the grid and programs that promote energy efficiency.

Looking ahead, while the EO was carefully drafted to avoid prejudging the outcome of the report, one can expect that if the report concludes that DLT will adversely impact the President's strategy for tackling climate change, there will be significant pressure on those that operate or invest in that technology to reduce or eliminate any adverse impacts before the technology is fully embraced by the federal government.

White Collar Crime

The Executive Order calls for an unprecedented focus of coordinated action across all relevant U.S. government agencies and with international partners to counter the criminal uses of cryptocurrency. Multiple agencies, including Treasury, State, the Department of Justice (DOJ), Commerce, Homeland Security, Office of Management and Budget, National Intelligence, and others, have the opportunity to submit a report to the President offering additional views on illicit financial risks posed by digital assets. These agencies are then required to develop "a coordinated action plan" that addresses "the role of law enforcement and measures to increase financial services providers' compliance with AML/CFT obligations related to digital asset activities." After the submission of these reports, the Secretary of the Treasury is expected to notify the relevant agencies of any "pending, proposed, or prospective rulemakings" aimed at curing illicit cryptocurrency risk.

While soliciting reports from the relevant departments and agency may not seem incredibly significant in itself, the EO's focus on rooting out crime on the blockchain is likely to resonate with the Justice Department and other regulators. In just the last month, the DOJ appointed the first director of its newly minted National Cryptocurrency Enforcement Team and announced the seizure of more than $3.6 billion in allegedly stolen cryptocurrency linked to the 2016 hack of Bitfinex.

With this EO, the scrutiny of cryptocurrency exchanges and other companies operating in this space is only likely to increase. These companies should expect to receive additional legal process and other requests for assistance in federal criminal investigations. They should also expect the DOJ to pay increased attention to their AML/CFT policies and procedures and their compliance with the Bank Secrecy Act.

You can subscribe to future advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

Kellen Dwyer
202.239.3240
212.905.9340
kellen.dwyer@alston.com

Blake E. Estes
212.210.9415
blake.estes@alston.com

Brian D. Frey
202.239.3067
brian.frey@alston.com

Byung J. "BJay" Pak
404.881.7816
bjay.pak@alston.com

Edward T. Kang
202.239.3728
edward.kang@alston.com

Kevin S. Minoli
202.239.3760
kevin.minoli@alston.com

Amy S. Mushahwar
202.239.3791
amy.mushahwar@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Cara M. Peterman
404.881.7176
cara.peterman@alston.com

Clifford S. Stanford
404.881.7833
cliff.stanford@alston.com

David S. Teske
404.881.7935
david.teske@alston.com

Alicia Badley
202.239.3636
alicia.badley@alston.com

ALSTON & BIRD

WWW.ALSTON.COM