ALSTON & BIRD

WWW.ALSTON.COM

Blockchain & Digital Assets ADVISORY ■

MAY 25, 2022

U.S. Government Steps Up Its Enforcement in the Digital Assets Space

Cryptocurrency is no longer on the fringe of the financial services industry. With over $1 trillion in market cap, star-studded Super Bowl ads, and an endless supply of frontpage headlines, there is no denying that crypto has entered the mainstream. The same is increasingly true for other digital assets and blockchain-based technologies, such as non-fungible tokens (NFTs). While the federal government largely took a "wait and see" approach to these emerging financial technologies over the last decade, the pace of enforcement activity by multiple agencies touching these spaces has been ramping up and filling the void caused by the absence of a comprehensive regulatory framework.

Following President Biden's Executive Order on Ensuring Responsible Development of Digital Assets issued in March (covered in a prior Alston & Bird advisory), there has been a flurry of enforcement activity touching all types of players in the industry, with serious implications for crypto exchanges, investors, promoters, service providers, and the companies that do business with them. There have been significant recent developments by a multitude of federal agencies and departments, including the Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), Department of Justice (DOJ), Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Consumer Financial Protection Bureau (CFPB), Office of Foreign Assets Control (OFAC), and Department of Labor (DOL). These agencies have used a variety of supervisory and enforcement tools to establish boundaries, send messages to the industry, and signal an appetite for future action, which we expect to continue at a rapid pace.

Securities and Derivatives (SEC/CFTC)

SEC expands crypto enforcement unit

On May 3, 2022, the SEC announced that it had nearly doubled the size of the specialized enforcement unit tasked with investigating and litigating alleged misconduct in the crypto markets. The newly renamed Crypto Assets and Cyber Unit now has 50 dedicated positions, including 20 new positions consisting of investigative staff attorneys, trial counsel, fraud analysts, and supervisors across the United States. The expanded unit will focus on investigating securities law violations related to: (1) crypto offerings; (2) crypto exchanges; (3) crypto lending and staking products; (4) decentralized finance (DeFi) platforms; (5) NFTs; and (6) stablecoins.

With a much deeper bench, a clear mandate to hunt down violations across a wide swath of the crypto-assets space, and a solid enforcement track record to support future actions, we expect even more vigorous enforcement by the SEC. The SEC's core crypto playbook was built on "regulation by enforcement," evidenced by more than 80 crypto-related enforcement actions since 2017, over $2 billion secured from defendants, and many novel fact patterns, including charges alleging that Poloniex operated an unregistered digital asset exchange, that Blockchain Credit Partners used smart contracts and DeFi technology to sell unregistered digital tokens, and that promoters of BitConnect's "lending program" failed to register as broker-dealers.

But the agency has also been broadcasting potential theories of liability in guidance issued over the last several years, and it may be emboldened because it deems crypto participants to be on more-than-ample notice. Examples include the 21(a) Report of Investigation on The DAO issued in 2017, the Framework for "Investment Contract" Analysis of Digital Assets issued in 2019, and Staff Accounting Bulletin No. 121 related to crypto disclosures issued in March. SEC leadership has repeatedly offered warnings as well, such as SEC Chair Gary Gensler's recent speech reiterating that "most crypto tokens are investment contracts under the Supreme Court's Howey Test" and therefore securities subject to SEC regulation.

More creative theories of liability may also be on their way. First, the SEC's expanded crypto unit helps fulfill the anti-crime/anti-fraud provisions of President Biden's Executive Order and is a way for the agency to keep pace with the "whole of government" approach and potentially assert its jurisdiction in gray areas. Second, the SEC recently proposed amendments to Regulation ATS that would sweep in "Communication Protocol Systems that make available for trading any type of security," potentially requiring crypto platforms and DeFi protocols to register as broker-dealers or exchanges. If finalized, these amendments would provide the SEC with access to far more information about the crypto markets and provide enforcement hooks for future actions. The SEC has now reopened the comment period for these amendments, and comments must be received on or before June 13, 2022.

SEC names crypto as an exam priority

On March 30, 2022, the SEC also named crypto-assets as an exam priority and "significant focus area" for 2022. The Division of Examinations emphasized that market participants involved in crypto-assets will be scrutinized on (1) their "offer, sale, recommendation, advice, and trading" of crypto-assets, "with a focus on duty of care and the initial and ongoing understanding of the products"; and (2) whether they "routinely review, update, and enhance their compliance practices …, risk disclosures, and operational resiliency practices" related to crypto custody arrangements, including "crypto-asset wallet reviews, custody practices, anti-money laundering reviews, and valuation procedures."

Broker-dealers, investment advisers, and other market participants should expect exam staff to shine a bright light on any involvement they have with crypto, which could lead to enforcement referrals if regulatory violations are uncovered. Market participants should not only pay close attention to the risk areas highlighted in the 2022 examination priorities but also consider revisiting the SEC's 2021 guidance on digital asset exams to understand other risk areas the SEC is scrutinizing.

We also expect the SEC to home in on market participants' interactions with retail investors in particular. For example, in the release announcing the expanded crypto unit, Enforcement Director Gurbir Grewal stated, "Crypto markets have exploded in recent years, with retail investors bearing the brunt of abuses in this space." In congressional testimony on May 17, 2022, Gensler also stated that "the highly volatile and speculative crypto marketplace has mushroomed, attracting tens of millions of American investors and traders," and "[t]he volatility in the crypto markets in recent weeks highlights the risks to the investing public."

CFTC and SEC coordinate their efforts

The CFTC has been active in crypto-related enforcement as well. On May 18, 2022, CFTC Chairman Rostin Behnam reportedly told an industry conference that the CFTC has filed more than 50 crypto-related actions since 2015 and is looking to prioritize this area with an influx of additional resources. As just one example of a recent high-profile action, on May 5, 2022 the CFTC announced that it had secured a $30 million civil money penalty against the co-founders of the Bitcoin Mercantile Exchange (BitMEX) crypto and crypto derivatives trading platform for alleged registration and anti-money laundering (AML) violations. This action notably occurred alongside a parallel criminal action, and the CFTC acknowledged the assistance provided by the U.S. Attorney's Office for the Southern District of New York and FinCEN.

Relatedly, Gensler revealed in a recent speech that he has asked SEC staff to "consider how best to register and regulate platforms where the trading of securities and non-securities is intertwined," and particularly "to work with the [CFTC] on how we jointly might address … platforms that might trade both crypto-based security tokens and some commodity tokens, using our respective authorities." The two agencies are reportedly developing memorandums of understanding related to their jurisdiction in the crypto space.

These developments show that government agencies are not hesitating to coordinate, even where their jurisdiction over the crypto markets is overlapping or unclear.

Criminal Enforcement (DOJ)

Through enforcement, policy, and resourcing, the DOJ continues to signal an unwavering focus on crypto-related matters and a continued expansion of the scope of crypto-related matters under investigation. Indeed, in remarks delivered at the February 2022 Munich Security Conference, Deputy Attorney General Lisa Monaco stated that the DOJ is "issuing a clear warning to criminals who use cryptocurrency to fuel their schemes. We also call on all companies dealing with cryptocurrency: we need you to root out cryptocurrency abuses. To those who do not, we will hold you accountable where we can."

The DOJ's recent enforcement actions demonstrate the wide range of areas where crypto-assets feature in DOJ investigations and prosecutions, and they serve as a reminder not only of the many threats companies with exposure to crypto-assets face but also of the extent to which compliance programs and other systems and controls must be designed and implemented with an eye toward ever-increasing areas of potential liability.

Notable recent DOJ crypto-related case developments

The DOJ has continued to investigate and prosecute significant numbers of cases involving cryptocurrency, including familiar fact patterns such as investment frauds and money laundering but also extending to newer areas such as sanctions evasion. Among the most notable DOJ crypto-related case developments around and after the issuance of the President's Executive Order are:

- **First criminal charges for using virtual currency to evade sanctions.** In May 2022, a federal magistrate judge in the District of Columbia issued an unsealed opinion (in an otherwise sealed case) that is believed to be the DOJ's first criminal prosecution of sanctions violations based on the use of virtual currency to evade sanctions. While many details of the case remain nonpublic, the court's opinion indicates that the DOJ has charged a defendant with conspiring to violate the International Emergency Economic Powers Act and defraud the United

States based on their transmission of over $10 million in virtual currency to a sanctioned country, and the court clearly endorsed the idea that sanctions violations using virtual currency may be criminally prosecuted.

- **Mining Capital Coin charges.** In May 2022, Luiz Capuci, the CEO and founder of cryptocurrency mining and investment platform Mining Capital Coin, was charged with a variety of federal fraud and money-laundering-related offenses arising from his alleged operation of a $62 million investment fraud scheme.
- **EminiFX charges.** In May 2022, Eddy Alexandre, the operator of purported cryptocurrency and foreign exchange investment platform EminiFX, was charged with commodities and wire fraud based on his alleged scheme to defraud investors of over $59 million.
- **BitMEX guilty pleas.** On March 9, 2022, the third co-founder of cryptocurrency derivatives exchange BitMEX, Samuel Reed, pleaded guilty to violations of the Bank Secrecy Act (BSA) arising out of his failure to establish, implement, and maintain an anti-money laundering program at BitMEX. His guilty plea followed February 24, 2022 guilty pleas by BitMEX's other co-founders, Arthur Hayes and Benjamin Delo.
- **Bitfinex hack charges and seizure.** In February 2022, Ilya Lichtenstein and Heather Morgan were charged with conspiracy to commit money laundering and conspiracy to defraud the United States in connection with their alleged laundering of $4.5 billion of cryptocurrency stolen from digital currency exchange Bitfinex's platform in a 2016 hack. Alongside the charges and the arrests of Lichtenstein and Morgan, the DOJ announced the seizure of more than $3.6 billion in cryptocurrency alleged to have been stolen in the hack, which has been described as the largest financial seizure in history.
- **BitConnect charges.** In February 2022, Satish Kumbhani, founder of purported cryptocurrency investment platform BitConnect, was charged with a variety of federal fraud and money-laundering-related offenses arising from his alleged operation of a $3.4 billion Ponzi scheme.

Notable DOJ organizational changes

Earlier this year, the DOJ installed new leadership and created new divisions that serve to propel its investigations and prosecutions in the cryptocurrency space.

- **Appointment of NCET director.** In February 2022, Eun Young Choi was named director of the DOJ's National Cryptocurrency Enforcement Team, an organization established in October 2021 and analyzed in a prior Alston & Bird blog post.
- **New DOJ initiatives.** In February 2022, Monaco announced the creation of a Virtual Asset Exploitation Unit at the FBI to "combine cryptocurrency experts into one nerve center that can provide equipment, blockchain analysis, virtual asset seizure, and training to the rest of the FBI." At the same time, Monaco announced the launch of an International Virtual Currency Initiative "to combat the abuse of virtual currency."

The foregoing is just a sampling of the many cases the DOJ continues to bring in crypto-related matters, and the volume of enforcement actions and investigative resourcing reflect a DOJ prioritization of crypto-related enforcement across subject-matter areas, from illegal narcotics to sanctions to investor protection. The DOJ's emphasis on these investigations and prosecutions is unmistakable and can be expected to continue and increase given the upward trend in crypto-asset utilization.

Federal Banking Agencies (OCC/FDIC)

OCC issues consent order against bank engaged in crypto custody

On April 21, 2022, the OCC issued a consent order against Anchorage Digital Bank, National Association, Sioux Falls, South Dakota, for its failure to adopt and implement an adequate BSA/AML compliance program. The consent order requires the bank to overhaul each of the pillars of its compliance program and to conduct a lookback for suspicious activity. In announcing the action, Acting Comptroller of the Currency Michael J. Hsu noted that the OCC will hold all nationally chartered banks to the "same high standards, whether they engage in traditional or novel activities."

The bank has only been subject to OCC regulation since it received conditional approval to convert from a South Dakota–chartered nondepository trust company in January 2021. At the time of the conversion, the trust company offered custody services primarily to institutional investors that transacted in digital assets and cryptocurrencies, as well as ancillary services. As a condition of approval, the trust company entered into an operating agreement with the OCC that spelled out, among other things, requirements related to BSA/AML compliance. The consent order specifically cited the bank's violation of these provisions of its operating agreement, highlighting the importance the agency placed on the conditions it set out for the trust company to obtain a charter. The timing of the action so quickly after the conversion suggests that it did not take long for the OCC to determine there were deficiencies that required more stringent oversight beyond the normal supervisory process.

While the OCC's willingness to grant charters to nontraditional financial entities has been the subject of ongoing discourse and even litigation, the consent order evidences the significant expectations that will be placed on entities trying to take advantage of a national charter's benefits in offering their crypto-related services. Given the potential money laundering, terrorist financing, and illicit concerns that President Biden and the Treasury Department have flagged with digital assets, BSA/AML compliance will likely take a position of paramount importance for those companies coming under OCC supervision. This consent order highlights the importance for companies seeking federal charters in understanding the nature and extent of federal banking supervision and the compliance improvements that may be necessary to ensure a smooth transition.

FDIC seeks notification from banks of crypto-related activities

On April 7, 2022, the FDIC issued FIL-16-2022 to its supervised institutions, advising them that they should "promptly" notify their regional directors if they currently engage in a crypto-related activity or, if they plan to engage in such an activity, before doing so. The notification should describe the activities "in detail" and allow the agency to assess the activities' safety and soundness, consumer protection, and financial stability implications. The FDIC notes that it will review the information and provide "relevant supervisory feedback" in a "timely manner." The agency may also request additional information from the bank as part of its evaluation.

Through this process, the FDIC has established a procedure that allows the agency to substantively evaluate proposed crypto-related activities under a supervisory microscope. The letter does not specifically detail what form the "feedback" may take, but one can imagine that the FDIC could impose nonpublic conditions or parameters on the activities based on its evaluation of the risk categories enumerated in the letter, each of which have malleable and nebulous definitions subject to significant agency discretion.

In addition, the evaluation process is not governed by any definite timelines, meaning that other proposed activities or even transactions could be held up until the FDIC completes its review. Targeted reviews can often uncover dormant issues of supervisory concern that quickly escalate into more serious actions against regulated banks. Thus, the FDIC's

newest procedure operates to give the agency a lot of flexibility to oversee crypto activities in the absence of any regulatory framework and employ any of its tools depending on the circumstances.

Additional analysis of the federal banking regulators' roadmap for crypto-asset regulation in 2022 is available in a previous Alston & Bird advisory.

Nonbank Consumer Finance (CFPB)

CFPB invokes authority to examine nonbank financial companies

On April 25, 2022, the CFPB announced that it is invoking a largely unused provision under the Dodd–Frank Wall Street Reform and Consumer Protection Act of 2010 to examine nonbank financial companies that the CFPB determines pose risks to consumers. The CFPB noted that entities subject to supervision based on risk are given notice and an opportunity to respond. The CFPB's announcement specifically noted that many nonbank financial companies—those entities that may now come under agency supervision—"brand themselves as 'fintechs.'"

Given CFPB Director Rohit Chopra's statements on the potential risks posed to consumers by cryptocurrency, it is likely that the CFPB will consider using this authority under Dodd–Frank to conduct examinations of, request records from, and potentially take actions against entities engaging in crypto-related activities. By activating this dormant authority, the CFPB's invocation may bring the agency off the sidelines and make it a more forceful participant in crypto enforcement going forward.

CFPB issues circular addressing deceptive representations of FDIC insurance

On May 17, 2022, the CFPB issued Consumer Financial Protection Circular 2022-02 stating the agency's view that misuse of the name or logo of the FDIC, or misrepresentations about deposit insurance, likely violate the Consumer Financial Protection Act's (CFPA) prohibition on deception. Importantly, the circular notes that a misrepresentation may violate the CFPA *even if* it was not made knowingly and further opines that disclaimers may not cure otherwise deceptive messages or practices. The circular advises that representations made about deposit insurance may be "particularly relevant" to digital assets, including crypto-assets, whose purveyors may try to entice consumers to use their products or services by advertising that they are FDIC-insured. The circular concludes that such firms "may be particularly prone" to making such deceptive claims about deposit insurance. In Chopra's statement accompanying issuance of the circular, he noted that the CFPB and FDIC are "especially concerned" about potential misconduct involving crypto-assets. The circular evidences another avenue through which the CFPB has entered the enforcement discussion for firms engaging in crypto-related activities.

Sanctions (OFAC)

OFAC confirms Russia sanctions cover virtual currency transactions

OFAC has been focused on the utilization of cryptocurrency as a means of sanctions evasion for several years, but the recent Russian invasion of Ukraine and related unprecedented sanctions has brought the issue to the forefront. In FAQ 1021, OFAC confirmed that Russia sanctions extend to virtual currency transactions. OFAC noted in particular that Russian sanctioned parties have been known to employ a wide variety of means to evade sanctions and that virtual currency businesses—including virtual currency exchanges, virtual wallet hosts, and other service providers, such as those that provide nested services for foreign exchanges—must be vigilant against circumvention attempts.

Although there was some initial speculation in the media that Russia would use cryptocurrency to fully or substantially blunt the impact of U.S. financial sanctions and to further support its war efforts, such concerns appear to have been largely unfounded. Nonetheless, companies that are subject to U.S. jurisdiction and that are involved in virtual currency transactions should view Russian-related transactions as being high risk from a compliance perspective.

OFAC lists virtual currency mixer on the SDN List

OFAC also continues to expand its utilization of the Specially Designated Nationals and Blocked Persons List (SDN List) to target sanctions evaders. On May 6, 2022, OFAC for the first time sanctioned a virtual currency mixer, Blender.io, for its involvement in supporting North Korean hacking and sanctions evasion. U.S. persons and entities are now prohibited from engaging in virtually any activity involving Blender and are required to block or freeze any property or interest in property—including cryptocurrency—that comes into such persons' or entities' possession or control. These developments follow on OFAC's publication of its Sanctions Compliance Guidance for the Virtual Currency Industry back in October 2021, covered in a prior Alston & Bird advisory. We expect increased scrutiny by OFAC on the cryptocurrency industry to continue.

Employee Benefits (DOL)

DOL issues guidance on crypto in 401(k) plans

Most private-sector retirement plans in the United States (including 401(k) plans) are subject to ERISA, which requires that plan fiduciaries act under the highest standard of care when investing plan assets or selecting investment options available under the plan. The DOL has the authority to investigate and enforce ERISA's fiduciary standards. On March 10, 2022, the DOL issued Compliance Assistance Release No. 2022-01 in which it cautioned ERISA plan fiduciaries to "exercise extreme care" before they consider adding a cryptocurrency option to a 401(k) plan's investment menu. The DOL said that cryptocurrencies pose significant risks and challenges to retirement accounts, including "risks of fraud, theft, and loss."

The DOL laid out that its concerns stem from its belief that (1) cryptocurrencies are highly speculative as investments; (2) 401(k) plan participants are less likely to make informed investment decisions on cryptocurrencies; (3) the methods of holding cryptocurrencies make them vulnerable to loss and hacking; (4) experts cannot agree on how to appropriately value cryptocurrencies; and (5) the evolving regulatory environment means that certain cryptocurrency transactions could be illegal, exposing plans and participants to liability and loss of protections. The DOL has said that plan fiduciaries that offer cryptocurrencies as investment options can expect to be questioned and investigated by the DOL.

Bitcoin investment option in 401(k) comes under scrutiny

On April 26, 2022, Fidelity Investments, one of the largest retirement plan providers in the country, announced that ERISA plan fiduciaries who use Fidelity to administer their 401(k) retirement plans will be able to add bitcoin as an investment option through a new Digital Access Account created by Fidelity. Fidelity would cap bitcoin investments to 20% of the participants' accounts, although plan fiduciaries could set a lower cap. Fidelity would initially allow investments only in bitcoin, but other digital assets could be added in the future. Fidelity is the second 401(k) plan recordkeeper (ForUsAll Inc. was the first) to offer access to cryptocurrency in a defined contribution retirement plan.

The DOL noted that it has "grave concerns with what Fidelity has done." Ali Khawar, acting assistant secretary of the Employee Benefits Security Administration, stated that cryptocurrencies are too speculative to be part of the retirement savings for the average American. Senators Elizabeth Warren (D-MA) and Tina Smith (D-MN) wrote a letter to Fidelity raising concerns about its move to allow bitcoin investments in 401(k) plans administered by Fidelity and asked Fidelity to respond to a series of questions.

Conclusion

This compilation of developments—while significant—represents only a sample of the expanding array of enforcement tools utilized by federal regulators in the digital assets space in recent months. And federal regulators are not alone. The states have also recently taken action in the digital assets space, including Guidance on Use of Blockchain Analytics issued by the New York Department of Financial Services in April and Executive Order N-9-22 signed by California Governor Gavin Newsom in May. Together, this array of activity demonstrates that digital assets and blockchain-based technologies are in the crosshairs of a wide range of government actors—and will likely remain there for the foreseeable future.

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 members of our Blockchain & Digital Assets Team:

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

Albert B. Stieglitz, Jr.
202.239.3168
albert.stieglitz@alston.com

Katherine Doty Hanniford
202.239.3725
kate.hanniford@alston.com

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

Blake C. MacKay
404.881.4982
blake.mackay@alston.com

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

Brendan Clegg
202.239.3237
brendan.clegg@alston.com

Jessica N. Garcia Keenum
404.881.4563
jessica.keenum@alston.com

Syed Fahad Saghir, A.S.A.
202.239.3220
fahad.saghir@alston.com

Matthew E. Newman
404.881.7987
matt.newman@alston.com

John O'Hara
212.210.9551
202.239.3131
john.ohara@alston.com

Matthew Bedford
202.239.3169
matthew.bedford@alston.com

ALSTON & BIRD

WWW.ALSTON.COM