BRACEWELL

INSIGHTS

DOJ Trumpets New Multi-Faceted Cryptocurrency Task Force: What this Means for You

October 26, 2021

By: ***Seth D. DuCharme***

In keeping with the United States government's expanding scrutiny of cryptocurrency markets, the DOJ recently ***announced*** the creation of a National Cryptocurrency Enforcement Team (the "NCET"). The NCET endeavors to add a layer of structure and coordination to the DOJ's investigative capabilities concerning illicit uses of cryptocurrency. According to Deputy Attorney General Lisa Monaco, the NCET will "tackle complex investigations and prosecutions of criminal misuses of cryptocurrency, particularly crimes committed by virtual currency exchanges, mixing and tumbling services and money laundering infrastructure actors." The creation of the NCET is an overt escalation of government involvement and enforcement in the cryptocurrency space. This demonstrates the Biden Administration's prioritization of general and specific deterrence for alleged misconduct in these emerging marketplaces.

Increased Cases Across Offices

The NCET's mandate is broad, blurring lines between traditional white collar and other federal crime and the emerging technologies associated with cryptocurrency and cyber-instrumentalities, neither of which are governed by clear, subject matter specific statutes. The NCET has been ***directed*** to "assist in tracing and recovering assets lost to fraud and extortion, including cryptocurrency payments to ransomware groups" and to pursue its own cases against entities that "enable the misuse of cryptocurrency and related products to commit or facilitate criminal activity." The volume of potential cases under this criteria is significant, but such cases are not easily made, due to the technologies associated with the transactions, as well as the often extra-territorial features of the underlying conduct, particularly in cybersecurity cases. These challenges mean that DOJ will aggressively and widely seek out information that may lead to viable prosecutions, and much of the burden in providing that information will fall on the parties who participate in the markets.

Initially, one should expect a surge of activities as the NCET finds its footing. Reportedly, the NCET has authority to pursue its own cases, in addition to supporting and coordinating existing and future cases brought by the various components in the DOJ's Criminal Division and in the U.S. Attorneys' Offices across the country. When the DOJ empowers and incentivizes such task forces, there are inevitable tensions and synergies among local offices, Main Justice components, and the investigative agencies that support them, as chain of command is established and tested. One result is an incentive for prosecutors and agents to a plant a flag in promising investigations to secure some measure of ownership and control of the case. This means faster action by DOJ elements as they try to build cases and meet senior leadership's

expectations to put points on the score board, fast. The issuance of more third-party subpoenas, subject and target letters, witness interviews, and scrutiny of public facing messaging are all foreseeable, and all can have immediate and costly consequences for stakeholders, particularly those who are unprepared.

Agencies Playing Well Together

In the announcement, the DOJ also emphasized its partnerships with other federal agencies, such as the Securities and Exchange Commission ("SEC") and the Commodity Futures Trading Commission ("CFTC"), in monitoring the cryptocurrency industry. This will further test the ability of the government to coordinate efforts and respect primacy among subject matter experts. While the DOJ frequently coordinates with the regulatory agencies, coordination initially can result in some confusion among outside parties, as they attempt to determine the correct agency or authority with whom to engage if proactive outreach is appropriate. This interagency approach to investigations is especially challenging when there is a whole-of-government drive to produce results in an area that is evolving both legally and technologically. The government will be anxious to show success in this regard.

Examined in the broader context, the recent announcement of the NCET is one in a series of efforts by the Biden administration to marshal U.S. regulators and law enforcement authorities to quickly and more aggressively focus on cyber technologies, particularly cryptocurrency. As we have reported previously, the Treasury Department's Office of Foreign Asset Controls issued an ***updated advisory*** and ***compliance guidance*** in September regarding the sanctions risks of facilitating ransomware payments using cryptocurrencies, raising the stakes for victims who make payments. Similarly, the SEC continues to aggressively review and pursue enforcement actions in the cryptocurrency space. From 2013 to 2020, the SEC brought 75 enforcement actions against cryptocurrency firms and individuals, ***resulting in $1.77 billion in penalties***.[1] It is by now well-established that the SEC views unregistered digital asset offerings, including ICOs, as viable targets for enforcement action.[2] For example, on August 9, the SEC ***announced*** a $10 million settlement with an online digital asset exchange for offering unregistered securities. The week before, SEC Chairman Gary Gensler ***stated*** that he agreed with his predecessor's view that "every ICO I have seen is a security."

The CFTC is also well established in regulating and enforcing this area. In 2015, the CFTC first ***determined*** that Bitcoin and other virtual currencies are properly defined as "commodities" under the Commodity Exchange Act ("CEA") and therefore subject to the CFTC's enforcement jurisdiction over commodities in interstate commerce.[3] The CFTC immediately followed up this announcement with its first enforcement case involving cryptocurrency and has been very active ever since. In fiscal year 2020 alone, the CFTC ***brought*** seven enforcement actions related to retail fraud in the cryptocurrency space. In October 2020, the DOJ and CFTC ***brought parallel proceedings*** against BitMEX, a cryptocurrency derivatives exchange. The allegations against BitMEX were for violations of the Bank Secrecy Act for its failure to maintain an adequate anti-money laundering program and for failing to register with the CFTC. Finally, in recent weeks, the CFTC has published separate settlements against major institutions involved in the cryptocurrency markets, including ***Kraken***, ***Bitfinex***, and ***Tether***, who the CFTC fined $41 million for making misleading statements about its U.S. dollar tether token. CFTC's statements associated with these enforcement orders indicate that the agency will continue to be aggressive in examining cryptocurrency markets and entities for violations of the CEA.

By DOJ embracing an all-of-government approach to policing cryptocurrency as it may relate to illicit activity, the risk assessment for companies involved in the cryptocurrency space has become more complex. Ideally, the end result of the multiagency approach to criminal enforcement will be better transparency and consistent integrity in what are quickly becoming key markets. In the short term, however, stakeholders can expect to bear some of the burden in satisfying the government's wariness of an evolving digital financial landscape.

Key Takeaways

With the creation of the NCET, a rise in enforcement actions, and the unleashing of U.S. regulators to dig deeper into emerging markets and the technologies that support them, the government has indicated that the cryptocurrency "grace period" is over. Stakeholders who are active in the cryptocurrency markets need to make sure that their regulatory due diligence will meet expectations and withstand scrutiny. This also means investing in employee training, monitoring tools for employees, market surveillance programs, broad compliance strategies, and "Know Your Customer" practices that account for the particular technical aspects and counterparties associated with digital transactions. These tools will assist firms in addressing and, if necessary, combating the government's now voracious appetite to reset the cryptocurrency landscape and deter misconduct by bringing in great numbers criminal cases, civil actions, and regulatory remedies. Cryptocurrency firms must be ready to respond to government requests or demands for information efficiently and accurately. By developing a regulatory risk assessment early, combined with robust compliance and surveillance programs, firms will be able confidently meet government investigators, and lawfully, successfully, and profitably navigate cryptocurrency-related ventures.

---

1. Of the SEC's 75 cryptocurrency-related enforcement actions from 2013-2020, 47 actions alleged fraud and 28 actions alleged an unregistered securities offering. Importantly, the SEC's enforcement actions based on fraud are ***historically aimed*** at true bad actors—entities defrauding investors, ICO fraud, etc.

2. In 2018, Judge Raymond Dearie issued a ruling rejecting arguments made in a motion to dismiss a criminal indictment that federal securities laws do not apply to cryptocurrencies. *See U.S. v. Zaslavskiy*, No. 1:17-cr-00647-RJD-RER (E.D.N.Y. Sept. 11, 2018). Judge Dearie's ruling was the first federal district court decision to rule that violations of federal securities laws were adequately alleged in connection with cryptocurrencies sold in ICOs and provides support to the SEC's position that federal securities laws apply to cryptocurrencies depending on the facts and circumstances.

3. This assertion by the CFTC has been upheld in some courts. For example, in March 2018, Judge Jack Weinstein issued a ruling that cryptocurrencies are commodities under the CEA and therefore subject to the CFTC's enforcement authority. *See Commodity Futures Trading Comm'n v. McDonnell*, No. 1:18-cv-00361-JBW-RLM, slip op. (E.D.N.Y. March 6, 2018). In September 2018, Judge Rya W. Zobel issued a ruling in a case alleging the fraudulent sale of cryptocurrency called My Big Coin. Judge Zobel ruled that the My Big Coin met the definition of a commodity, and thus fell under the jurisdiction of the CFTC, allowing the regulator to pursue fraud charges involving the cryptocurrency. *See Commodity Futures Trading Comm'n v. My Big Coin Pay, Inc.*, No. 1:18-cv-10077-RWZ (D. Mass. Sept. 26, 2018).