New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 266—NO. 103
MONDAY, NOVEMBER 29, 2021

Outside Counsel

Biden Administration Increasingly Focused on Crypto Exchanges

By **Ilene Jaroslaw**

And **Matthew L. Levine**

Over the last half decade, as the value of cryptocurrencies such as Bitcoin and Ethereum has skyrocketed, the associated coins and tokens have become not just means of payment but speculative investments traded among investors. This activity has led to increased interest from federal agencies, which seek to protect investors from fraud and the public from money-laundering by targeting traders and coin developers.

More recently, the federal government is taking aim at the centralized and decentralized exchanges where cryptocurrencies are traded. As ransomware attacks, such as the one that shut down the Colonial Pipeline, increasingly cause victims to acquire cryptocurrencies to pay ransom, federal prosecutors and regulators have begun taking a hard look at this ecosystem. In particular, the Biden Administration has increasingly focused on cryptocurrency exchanges by ramping up its monitoring and enforcement across various agencies. This article will review some recent developments at these regulatory and prosecutorial agencies.

DOJ Investigations

In October 2020, the Department of Justice (DOJ) charged the founders of Seychelles-based BitMEX, an exchange that traded in futures and derivatives of cryptocurrencies, with violations of the Bank Secrecy Act for inadequate anti-money laundering controls. That same month, DOJ published its first "Cryptocurrency Enforcement Framework," which concluded by emphasizing that the agency will continue with "aggressive investigation and prosecution of a wide range of malicious actors [in the cryptocurrency space], including those who use cryptocurrencies to commit, facilitate, or conceal their crimes."

A year later, DOJ looks to have delivered on this promise. For example, this year it charged a Russian citizen for allegedly violating anti-money laundering compliance and licensing laws by operating a cryptocurrency mixer designed to conceal cryptocurrency transactions on the darknet, appropriately named "Bitcoin Fog." Bitcoin Fog actually advertised to potential users that its mixer would "mak[e] it impossible to prove any connection between a deposit and a withdrawal inside our service."

This was followed recently by a guilty plea from another individual who operated a different mixer, called "Helix," for engaging in a conspiracy to launder money in connection with one of the largest darknet markets, AlphaBay.

Additionally, it was reported in May 2021 that DOJ and the Internal Revenue Service together began

ILENE JAROSLAW *is chair of the white-collar criminal defense practice at Phillips Nizer. She previously served as a federal prosecutor in the Eastern District of New York and a senior staff attorney at the Center for Reproductive Rights.* MATTHEW L. LEVINE *is also a partner at the firm. He previously served as a federal prosecutor in both the Eastern District of New York and Washington D.C., and as the First Executive Deputy Superintendent for Enforcement at the New York State Department of Financial Services. Associate* JEREMY BACHRACH SIEGFRIED *assisted in the preparation of this article.*

investigations of Binance, one of the largest cryptocurrency exchanges, apparently over concerns involving potential money-laundering and tax evasion. This follows a report by blockchain analytics firm Chainalysis, which determined that more than a quarter of Bitcoin transactions linked to suspicious activity moved through the Binance exchange. (*Bloomberg*, May 13, 2021)

Another report indicated DOJ is investigating the companies that together issue and offer Tether, a stablecoin, concerning allegations that Tether may have concealed from banks that certain of its transactions were linked to cryptocurrency. Tether, according to the New York Attorney General, is owned and operated by the same group of executives and employees who operate Bitfinex, another one of the largest cryptocurrency exchanges. The recent reporting notes that DOJ has notified certain individuals that they are targets of the investigation, indicating the inquiry may be in advanced stages. (*Bloomberg*, July 26, 2021)

And in June 2021, DOJ investigative efforts resulted in the successful recovery of $2.3 million in Bitcoin representing the proceeds of the damaging ransomware hack that shut down operations of natural gas operator Colonial Pipeline for many days.

In recent weeks DOJ has signaled that it is accelerating its push into cryptocurrency enforcement with a particular focus on exchanges. In back to back speeches, Deputy Attorney General Lisa Monaco, and Principal Associate Deputy Attorney General John Carlin, both indicated that DOJ was ramping up its focus on crimes around cryptocurrency exchanges. Deputy Attorney General Monaco announced DOJ had formed the National Cryptocurrency Enforcement Team (NCET), tasked with monitoring cryptocurrency exchanges and other parts of the blockchain infrastructure that facilitate ransomware payments and money-laundering. The Deputy Attorney General took pains to note that DOJ's NCET will focus on "crimes committed by virtual currency exchanges," as well as mixing and tumbling services and other money laundering infrastructure actors.

Where previous enforcement efforts by federal agencies have tended to focus on digital coins, coin developers, and traders, under the new leadership of the Biden Administration, there is now a greater focus on cryptocurrency exchanges.

Similarly Carlin made clear that those cryptocurrency exchanges and peer-to-peer lending platforms where abundant illicit financing takes place will be squarely in DOJ's crosshairs, as this is where the illicit "conversion occurs, and [DOJ will] hold[] accountable and responsible those who facilitate those conversions so we can best safeguard the financial system and the American public."

Regulatory Enforcement by The SEC and CFTC

The SEC: New Chair Gary Gensler has made abundantly clear that cryptocurrency is at the very top of the SEC's enforcement priorities, and that cryptocurrency exchanges are fair game. For example, Gensler, in a recent magazine interview, discussed "trading and lending platforms," stating, "[t]he big ones now have trading on 50 or 200 tokens, and probabilities are such that many of those tokens are securities or investment contracts under our laws. It would be far better if some of these platforms came in and actually registered as to what they are …. [T]hey work best when they're in some regulatory perimeter." These comments followed on the heels of other public remarks in which he suggested that the cryptoverse was like the "Wild West." Gensler expressed concern about the use of cryptocurrency to facilitate ransomware extortion, and signaled interest in investigating the roles of cryptocurrency exchanges in unregistered offerings for stablecoins.

Gensler's comments reflect an already strong emphasis by the agency on cryptocurrency enforcement. Even before Gensler's confirmation in April, the SEC in February 2021 issued a subpoena to the DeFi Money Market, a large cryptocurrency exchange in the "decentralized finance" cryptocurrency arena. Although the focus of the subpoena is unclear, it is a meaningful signal that the SEC is moving more aggressively to regulate exchanges. Then, in September 2021, it was reported that the SEC had hired AnChain. AI, another blockchain analytics company, specifically to monitor exchanges.

And only days later, the Wall Street Journal reported that the SEC is investigating UniSwap Labs, described as "the main developer of the world's largest decentralized cryptocurrency exchange." While the precise focus of the investigation remains known, it is yet another example of the SEC's interest in targeting exchanges in the name of investor protection.

The CFTC: The CFTC also continues to flex its regulatory muscle against cryptocurrency exchanges. It recently issued an order against Bitfinex, the exchange closely associated with Tether. According to the CFTC's allegations, Bitfinex and Tether commingled funds—something that its public filings allegedly failed to disclose—thereby causing the Tether stablecoin to lose value.

Additionally, although a 2016 CFTC Order prohibited Bitfinex from permitting certain U.S. non-Eligible Contract Participants to trade on its platform, the CFTC investigation determined that Bitfinex's Know-Your-Customer (KYC) and due diligence procedures were inadequate to filter out these participants. The CFTC further found that Bitfinex knew its KYC and due diligence programs were deficient and nonetheless chose not to undertake remediation. Bitfinex paid a $1.5 million penalty for its conduct.

OFAC Enforcement

The Office of Foreign Assets Control (OFAC) is also stepping up its enforcement game to include cryptocurrency exchanges. It took its first ever action against an exchange when it imposed sanctions on Suex OTC S.R.O, a large international cryptocurrency exchange, adding it to the sanctioned entity list. OFAC took this action after determining that the exchange played a significant role in facilitating transactions involving illicit proceeds from at least eight ransomware variants; it found that over 40 percent of SUEX's known transaction history was associated with illicit actors. Making clear its focus on exchanges will continue,

Exchanges and their operators therefore must be vigilant in monitoring activity on their platforms, and must implement robust compliance programs.

Deputy Treasury Secretary Wally Adeyemo asserted that, "Exchanges like Suex are critical to attackers' ability to extract profits from ransomware [victims]."

Takeaways: Emphasis On Strong Compliance

Where previous enforcement efforts by federal agencies have tended to focus on digital coins, coin developers, and traders, under the new leadership of the Biden Administration, there is now a greater focus on cryptocurrency exchanges. For exchange owners and operators, this means the potential for increased liability for use of their platforms for money laundering, ransomware attacks, funding of terrorist activities, unregulated activity, and investor harm.

Exchanges and their operators therefore must be vigilant in monitoring activity on their platforms, and must implement robust compliance programs. This is a key take away from the recent comments of both Deputy Attorney General Monaco and PDAG Carlin. Carlin stated last month: "We're going to continue to increase the burden on both those who operate those cryptocurrency exchanges, have the same type of KYC culture that you've had in banks … . We have a broad range of legal authorities and we're going to use an all-tools approach to dealing with cryptocurrency-related crime."

Monaco's most recent policy statement, on Oct. 29, 2021, warned that companies must take a proactive role in ensure that criminal activity on their platforms is prevented, detected, and thwarted. She announced a renewed focus on corporate crime, with corporations and their bad actors both subject to prosecution, with this warning: "Companies need to actively review their compliance programs to ensure they adequately monitor for and remediate misconduct—or else it's going to cost them down the line."