November 8, 2021

Increased Scrutiny for the Crypto Industry: DOJ Creates a Special Enforcement Team as Regulators Sharpen their Focus

Christian R Everdell; Barbara K Luse

The cryptocurrency industry should brace itself for increased scrutiny from the Department of Justice ("DOJ") and other enforcement agencies. On October 6, 2021, the DOJ announced the creation of a National Cryptocurrency Enforcement Team ("NCET"). According to the announcement, the team will have the authority to tackle "investigations and prosecutions of criminal misuses of cryptocurrency, particularly crimes committed by virtual currency exchanges, mixing and tumbling services,[1] and money laundering infrastructure actors."[2] The NCET will also assist in the tracing and recovery of assets lost to fraud and extortion, including cryptocurrency payments made to ransomware groups.

The announcement suggests that the NCET's initial mandate will broaden the enforcement focus from criminal actors themselves to those who enable and facilitate illicit activities involving cryptocurrency. Who does this potentially mean? Cryptocurrency exchanges, for one. The DOJ announcement focused on exchanges, noting that the NCET will strengthen the DOJ's capacity to "dismantle the financial entities that enable criminal actors to flourish — and quite frankly to profit — from abusing cryptocurrency platforms."[3] But the increased scrutiny will also likely extend to all cryptocurrency-focused businesses, non-fungible token ("NFT") platforms, companies that accept cryptocurrency as payment, and even those that merely do business with third parties dealing in cryptocurrency.

Specifics of the NCET Mandate

Assistant Attorney General Kenneth A. Polite Jr. will supervise the NCET, which will combine the expertise of the DOJ's Criminal Division's Money Laundering and Asset Recovery Section ("MLARS"), the Computer Crime and Intellectual Property Section ("CCIPS") and other sections in the division, with experts brought in from United States Attorneys' Offices ("USAOs").[4]

The DOJ announcement provides that the NCET will build upon MLARS's Digital Currency Initiative and the team's approach will be "informed by" the Department's Cryptocurrency Enforcement Framework

[1] Mixing and tumbling services break the connection between the wallet address sender and the recipient address. The process is designed to allow the source of the funds to remain anonymous.

[2] *See* "Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team," October 6, 2021. https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team

[3] *Id.*

[4] *Id.*

("Framework"), released in October 2020 under former Attorney General William Barr. Under the Framework, the DOJ's enforcement activity focuses on "illicit" uses of cryptocurrency, which typically fall under three broadly defined categories:

1. Financial transactions associated with the commission of crimes or in support of terrorism.
2. Money laundering and the shielding of legitimate activity from tax, reporting, or other legal requirements.
3. Direct commission of crimes, such as theft and fraud, that implicate the cryptocurrency marketplace.[5]

It is not difficult to see how the first category, in particular, could provide a catch-all for any transactions linked to illicit uses of cryptocurrency, however remote the link. Significantly, the Framework also emphasizes the importance of interagency partnerships with regulatory agencies such as the Financial Crimes Enforcement Network ("FinCEN"), the Office of the Comptroller of the Currency ("OCC"), the Securities and Exchange Commission ("SEC"), and the Commodity Futures Trading Commission ("CFTC").[6]

Collaboration with Other Enforcement Authorities

The DOJ announcement provides that the NCET will not only pursue its own cases but will "support existing and future cases brought across the Criminal Division and in the U.S. Attorneys' Offices across the country."[7] The announcement specifies that the NCET will work closely with other federal agencies, subject matter experts, and its law enforcement partners throughout the government.

The SEC will undoubtedly be part of that collaboration. The creation of the NCET comes at a clear inflection point for the SEC's enforcement and regulation of digital assets in the United States and around the world. The first futures-based Bitcoin exchange-traded fund ("ETF"), ProShares Bitcoin Strategy ETF, began trading on the New York Stock Exchange in mid-October, and a second, Valkyrie Bitcoin Strategy Fund, was listed on the Nasdaq Exchange a few days later. These events represent clear milestones for the industry, which has been pushing regulators for years to approve a Bitcoin ETF.[8] Despite these advances, SEC Chairman Gary Gensler has expressed concern and signaled an intent to ramp up regulation and enforcement. Chairman Gensler has warned of the SEC's intention to more actively police the cryptocurrency market, which he has referred to as the "Wild West" and "rife with fraud, scams, and abuse."[9] The day before the DOJ's announcement about the NCET, Chairman Gensler

[5] See "Cryptocurrency Enforcement Framework," Report of the Attorney General's Cyber Digital Task Force, October 2020. https://www.justice.gov/archives/ag/page/file/1326061/download

[6] *Id.*

[7] *See* "Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team," October 6, 2021. https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team

[8] To date, regulatory approval has only been granted for Bitcoin futures ETFs as opposed to a Bitcoin spot ETF.

[9] *See* "Chair Gary Gensler Testimony Before the United States House of Representatives Committee on Financial Services," October 5, 2021. https://www.sec.gov/news/testimony/gensler-2021-10-05

testified before the House of Representatives Committee on Financial Services where he repeated his call for greater investor protection and reiterated the SEC's commitment to collaborating with other federal agencies.[10]

Regulatory rumblings can also be heard from the CFTC, which has been sharing crypto regulatory oversight responsibility with the SEC and FinCEN. Recently, the acting chair of the CFTC said in a speech before the Senate Agriculture Committee that if he is confirmed for a full term in the chairmanship, the CFTC could act as a "primary cop on the beat" for the cryptocurrency market.[11]

The DOJ has already undertaken several successful cryptocurrency enforcement actions in collaboration with other regulatory agencies. The DOJ recently collaborated with FinCEN on joint criminal and civil enforcement actions against Larry Dean Harmon, the operator of Bitcoin mixer, Helix.[12] The DOJ also collaborated with FinCEN and the CFTC against the cryptocurrency derivatives trading platform BitMEX.[13] NCET will likely continue this sort of work in coordination with other regulatory agencies that have all said they will make crypto a priority. Indeed, just recently, a group of senior attorneys from the DOJ, SEC, and CFTC speaking at the annual ABA White-Collar Crime conference emphasized that cryptocurrency cases would be a priority.[14]

NCET at the Junction of Crypto, Money-Laundering, and Cybercrime: What's on the Horizon

The DOJ's avowed focus on exchanges and infrastructure providers corresponds to a moment when the link between cryptocurrencies, money-laundering and cybercrime has come to the forefront with high-profile targets including infrastructure (Colonial Pipeline Co.), universities, hospitals, and even the Texas state judiciary.

Virtual currency exchanges often play an integral role in ransomware and cyber-attacks because of their facilitation of ransomware payments and money-laundering activities. In September, the U.S. Department of the Treasury ("Treasury") listed the first virtual currency exchange, SUEX OTC, S.R.O. ("SUEX") as a Specially Designated National ("SDN"). Treasury accused SUEX of helping cybercriminals convert funds into fiat currency.[15] Although the Russia-based SUEX may have been a low hanging fruit,[16]

---

[10] *Id.*

[11] *See* "CFTC Should Be Crypto's 'Primary Cop,' Acting Chairman Says," October 27, 2021. CFTC Should Be Crypto's 'Primary Cop,' Acting Chairman Says (coindesk.com)

[12] *See* "Ohio Resident Charged with Operating Darknet-Based Bitcoin "Mixer," which Laundered Over $300 Million," February 13, 2020. https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million

[13] *See* "Federal Court Orders BitMEX to Pay $100 Million for Illegally Operating a Cryptocurrency Trading Platform and Anti-Money Laundering Violations," August 10, 2021. https://www.cftc.gov/PressRoom/PressReleases/8412-21

[14] *See* "Top Enforcement Officials Eye Individual Prosecutions, Crypto," October 27, 2021. Top Enforcement Officials Eye Individual Prosecutions, Crypto - Law360

[15] *See* "Treasury Takes Robust Actions to Counter Ransomware," September 21, 2021. https://home.treasury.gov/news/press-releases/jy0364

[16] In its press release, Treasury reported that over 40% of SUEX's known transaction history was associated with illicit actors.

Treasury's decision to add the exchange to the government's sanctions list signals a broader focus on facilitators of ransomware attacks, rather than solely on the attackers themselves.

On October 15, 2021 – just about one week after the DOJ's launch of the NCET – Treasury's Office of Foreign Assets Control ("OFAC") issued guidance aimed at promoting sanctions compliance in the virtual currency industry.[17] OFAC has reiterated that its sanctions compliance requirements apply to the virtual currency industry in the same way they apply to traditional financial institutions. Coupled with these recent moves at Treasury, the DOJ's launch of the NCET suggests that other exchanges may soon find themselves on the government's sanctions list.

It also bears mention that the DOJ's launch of the NCET came on the same day that the Department launched its Civil Cyber-Fraud Initiative to combat "new and emerging cyber threats to the security of sensitive information and critical systems."[18] The NCET and Civil Cyber-Fraud Initiative will likely work hand-in-hand towards the goal of "enhance[ing] and expand[ing]" the Department's efforts against cybercrime.

Who Should Seek Counsel?

It seems clear that cryptocurrency exchanges are being placed under the microscope, and they should take appropriate steps to work with counsel to avoid becoming the subject of a DOJ investigation or prosecution. But with heightened scrutiny from the DOJ and a constantly evolving regulatory landscape, all companies in the industry should evaluate compliance programs and practices to mitigate risk and exposure.

Crypto funds and financial institutions should re-evaluate their anti-money laundering ("AML") and Know Your Customer ("KYC") compliance programs to ensure that their AML and KYC programs adequately account for cryptocurrency-related exposure.

Fintech startups in the space should also make sure to implement appropriate compliance programs, even in the early stages.

NFT marketplaces have cause for concern as the platforms have already shown themselves to be ripe for money laundering and fraud due to the relative anonymity of users and the fact that NFTs are bought and sold using cryptocurrencies.

Finally, all companies invested in cryptocurrency should take steps to ensure that they are adequately protected from risks associated with their investment in the asset class. Companies that do find themselves under investigation should make sure to seek counsel with strong regulatory and criminal enforcement experience.

[17] *See* "Sanctions Compliance Guidance for the Virtual Currency Industry," Office of Foreign Assets Control, October 2021. https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf

[18] *See* "Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative," October 6, 2021. https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative

The Authors:

Christian E Everdell
Partner

+1 212 707 7268
ceverdell@cohengresser.com

Barbara K Luse
Associate

+1 212 707 7265
bluse@cohengresser.com

About Cohen & Gresser:

Cohen & Gresser is an international law firm with offices in New York, Paris, Washington, DC, and London. We have an outstanding record of success in high-stakes and high-profile litigation, investigations, transactional and government relations work for our clients, including major financial institutions and companies across the world. Our attorneys have superb credentials and are committed to providing the efficiency and personal service of a boutique law firm along with the quality and attention to detail that are the hallmarks of the best firms in the world. The firm has been recognized in a wide range of publications, including *Chambers* and *The Legal 500*.

New York | Paris | Washington DC | London

www.cohengresser.com
info@cohengresser.com
+1 212 957 7600

View C&G's Profile