PAUL HASTINGS

Stay Current

February 2022

Follow @Paul_Hastings

NCET Spells a New Phase of Crypto Enforcement

By Laurel Loomis Rimon & Braddock Stevenson

Key Takeaways:

- The NCET Director announcement is an important step in the DOJ's ongoing initiative to aggressively disrupt and prosecute cryptocurrency crime through significant investments in personnel, resources, and inter-agency and cross-border coordination.
- The DOJ is emphasizing corporate compliance with Bank Secrecy Act and Anti-Money Laundering requirements, with a particular focus on entities that facilitate cryptocurrency crimes.
- The NCET and related initiatives will enhance international evidence-sharing and cooperation and coordination with domestic regulatory agencies.
- The NCET can be expected to aggressively pursue unlicensed money transmitting and money laundering prosecutions, as well as significant forfeitures of cryptocurrency tied to criminal activity.
- As law enforcement efforts against corporate actors intensify, companies receiving information requests and subpoenas, including third-party subpoenas, should take specific steps when interacting with law enforcement related to suspicious transactions.

Last week, the Department of Justice named the Director of its recently-formed National Cryptocurrency Enforcement Team (NCET), marking another step forward in the DOJ's cryptocurrency enforcement strategy. Eun Young Choi, a former Southern District of New York prosecutor and Senior Counsel to Deputy Attorney General Lisa Monaco, will be the first Director of the NCET. Choi is an experienced prosecutor with specialized experience handling cyber hacks and virtual currency cases, and her selection highlights the intensity of the DOJ's focus in building out a crypto-specific enforcement team that will investigate and prosecute its own cases while also supporting the efforts of U.S. Attorney's offices nationwide. This announcement was accompanied by news of the FBI's new Virtual Asset Exploitation Unit (VAXU), which will work with the NCET and is designed to be a central resource for FBI agents around the country for technical assistance and training related to blockchain analysis and asset seizures.

These teams are expected to increase the focus on corporate misconduct, specifically including cryptocurrency exchange activity, unhosted wallet applications, and cryptocurrency marketplaces. Decentralized Finance applications will not be immune. Individual and corporate prosecutions, as well as high-value forfeiture actions, are expected to increase as a result of DOJ's initiative. Companies

engaging with cryptocurrency will need to demonstrate that they are employing serious compliance programs customized to the particular risks in the blockchain ecosystem, and will want to employ transaction monitoring systems that allow them to identify illicit activity on their platforms.

The NCET's New Tools

With the NCET Director now in charge of a team of prosecutors dedicated to cryptocurrency crimes, the DOJ is expected to be more aggressive and strategic in its investigations and prosecutions in this space. Being housed in DOJ's headquarters Criminal Division rather than in any particular U.S. Attorney's office, the NCET should have access to more dedicated resources to investigate and prosecute what are typically document and resource-intensive cases.

Like other efforts managed out of the Criminal Division, the NCET will proactively engage and coordinate with federal, state, and local agencies, including civil regulators such as the SEC, CFTC, and FinCEN, pulling together leads from various investigations, and sharing information. The NCET can also be expected to collaborate with international agencies around the world and participate in coordinated enforcement actions across jurisdictions. In public remarks discussing Director Choi's appointment, Deputy Attorney General Monaco emphasized that, as the vast majority of cybercrimes are international in scope, the DOJ will be making international coordination and evidence-gathering a routine part of its virtual currency investigations.

Enforcement Building Blocks

To date, DOJ's enforcement efforts in the cryptocurrency space have primarily targeted those complicit in underlying criminal activity such as corrupt exchanges founded with stolen funds, mixers facilitating anonymous transfers of cryptocurrency across blockchains, and individuals providing illicit services on darknet marketplaces. As early as 2007, and through more recent years, purported "unregulated" and "untouchable" online marketplaces and virtual currency exchanges like e-gold, the Silkroad, AlphaBay, and BTC-e have all been subject to DOJ prosecution and forfeitures, but these involved targets who were themselves egregious actors. The Department's BitMex indictment in the fall of 2020 was a milestone, where corporate principals were individually indicted for pure anti-money laundering compliance failures.

This month's multi-billion dollar DOJ seizures and arrests associated with the Bitfinex hack are another turning point. Although a single case that has not yet been litigated, this action placed the Department's use of blockchain analytics protocols front and center. This case demonstrated the DOJ's ability to identify individual actors conducting transactions on a public blockchain through the use of industry-available software tools that identify connections between people and transactions through the automated analysis of large data sets. The magistrate judge who issued the seizure warrant reviewed and validated the use of these tools for the purpose of establishing probable cause. A facility with blockchain analytic tools is now essential for law enforcement, the judiciary, and cryptocurrency companies.

DeFi: A Novel Industry Should Expect Novel Prosecutions

"Decentralized" platforms will not be off-limits to prosecutors. On the regulatory front, FinCEN's 2019 cryptocurrency guidance suggested that the creators of decentralized applications could potentially fall within the reach of federal money transmitter laws, extending AML program requirements to DeFi platforms. Where criminal money laundering is concerned, DOJ will be looking behind a decentralized structure to identify parties who fit any of the following categories as potential targets: those who are profiting substantially while avoiding regulatory requirements; those funneling their customers into

decentralized payment methods to avoid scrutiny; those designated by the community to manage compliance; and those who developed smart contracts to facilitate decentralized payments. Cryptocurrency platforms and marketplaces that rely on Decentralized Finance applications should ensure that they are not the lowest hanging fruit for DOJ by implementing AML compliance best practices to avoid becoming a haven for suspicious transactions.

When a Subpoena Arrives . . .

> "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."
>
> —Deputy Attorney General Monaco, Munich Security Conference, February 17, 2022

Many of the cryptocurrency investigations noted above were built on information provided through third-party subpoenas issued to unnamed cryptocurrency platforms. As DOJ becomes more proficient in blockchain investigations, it will inevitably look to cases that will move the needle for BSA and AML compliance within the mainstream cryptocurrency industry. In particular, the DOJ can be expected to seek out exchanges or other platforms that act as common cash-out points for illicit actors, with an eye to whether regulated financial institutions failed to identify and report suspicious information required by the BSA. Unique to the current wave of online financial services, the exponential growth that can be quickly generated by new blockchain platforms creates significant compliance challenges and risks, often providing law enforcement an easy pressure point.

In light of the DOJ's heavy reliance on summary blockchain analytics as evidence to support significant action, recipients of subpoenas—third party or otherwise—should consider the following:

- Law enforcement requesters often need to be educated about what portion of the subject activity is, or is not, readily visible on the blockchain and/or subject to particular blockchain analytics tools;
- Regulators expect a subpoena to trigger an investigation into whether the filing of a Suspicious Activity Report (SAR) is necessary;
- A subpoena may indicate a need to review your exposure to the subject and the alleged conduct, and to determine the company's role as a counterparty, pass-through or layering vehicle, or cash-out point;
- A subpoena may be a basis to review whether earlier blockchain alerts or other indicators suggest a SAR should have previously been filed;
- Other accounts outside the scope of the subpoena, but related to the subject or activity, may need review, a SAR filing, or other action; and
- You may need to evaluate existing monitoring rules and policies that failed to identify suspect behavior.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact either of the following Paul Hastings Washington, D.C. lawyers:

Laurel Loomis Rimon
1.202.551.1889
laurelrimon@paulhastings.com

Braddock Stevenson
1.202.551.1890
braddockstevenson@paulhastings.com