Westlaw Today
powered by Reuters

Insider trading and NFTs

By Mary Kuan, Esq., Joshua K. Bromberg, Esq., and Jared R. Gianatasio, Esq., Kleinberg, Kaplan, Wolff & Cohen PC*

JUNE 22, 2022

On June 1, 2022, the United States Attorney for the Southern District of New York and the Assistant Director-in-Charge of the New York Field Office of the Federal Bureau of Investigation announced the unsealing of a two-count indictment for wire fraud and money laundering against Nathaniel Chastain, a top executive at Ozone Networks, Inc., d/b/a/ OpenSea (OpenSea), self-described as the world's first and largest NFT marketplace.

NFTs or "non-fungible tokens" are digital assets that can be used to denote ownership of art, music, sports memorabilia, in-game items, or videos.

The government's indictment sidesteps the issue of whether the NFT is a security, as the indictment is for insider trading under wire fraud and money laundering laws, rather than the securities laws.

If convicted, Chastain faces a maximum sentence of 20 years' imprisonment, as well as the forfeiture of all proceeds from the commission of the crime, including from his personal property.

The indictment is a landmark event, marking the first time that U.S. federal prosecutors have brought "insider trading" charges in connection with digital assets and heralding the potential for increased and expanded enforcement actions and regulations in this space.

In light of this case, it may be prudent for digital asset platforms, investment firms, and other market participants investing in or involved with digital assets to consider either implementing compliance and insider trading policies or reviewing their existing compliance and insider trading policies, as well as to consider analyzing whether particular NFTs may constitute securities.

Allegations

The government's indictment alleges that (i) the price of NFTs typically increased after featuring on OpenSea's homepage, (ii) Mr. Chastain was responsible for selecting the NFTs that were to be featured on OpenSea's homepage and therefore knew, in his capacity as an employee of OpenSea and on a confidential basis, what would be featured before the general public, and (iii) for at least three months, Mr. Chastain misappropriated such confidential information by secretly purchasing such NFTs prior to their feature on the website and selling such NFTs after their feature for significant profits by using anonymous digital currency wallets and anonymous accounts on OpenSea.

We note that the government's indictment sidesteps the issue of whether the NFT is a security, as the indictment is for insider trading under wire fraud and money laundering laws, rather than the securities laws.

While this may signal some ambivalence or uncertainty regarding the regulatory scheme applicable to NFTs, it is notable that that certain platforms are independently performing analysis as to whether NFTs constitute securities.

It is also notable that the U.S. Securities and Exchange Commission (SEC) recently announced its desire to review the NFT market, including NFT content creators and crypto exchanges where NFTs are traded, for purposes of determining whether some NFTs should be regulated as securities under U.S. securities laws and whether platforms that facilitate NFT trading should be deemed securities exchange platforms.[1]

Earlier this year, the SEC's enforcement division issued subpoenas to a number of NFT firms requesting further information on a variety of issues, including further information on so-called "fractional NFTs," which involve breaking down the underlying assets into "units" that can be easily bought and sold.

In addition, in October, 2021, OpenSea disabled trading of "DAO Turtles" for breaking its terms of service for "creating, listing, or buying securities, commodities, options, real estate, or debt instruments."

Insider trading nearly always has been charged under the robust line of case law developed from Section 10(b) of the Securities Exchange Act of 1934, as amended, and Rule 10b-5 promulgated under the act.

The act prohibits "in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered, or any securities-based swap agreement any manipulative or deceptive device or contrivance in contravention

of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors."[2]

A criminal violation of the statute necessarily requires that the "manipulative or deceptive device or contrivance" be in connection with a purchase or sale of a "security" or a "securities-based swap agreement."

Parties involved in digital assets may consider it wise to have robust protocols to detect and prevent "insider trading" similar to what has largely been adopted in the context of securities trading.

In situations where a "security" may not be involved, the Department of Justice can also bring a fraud claim under the wire fraud statute, which is more general and "reach[es] any scheme to deprive another of money or property by means of false or fraudulent pretenses, representations, or promises"[3] if such scheme is carried out "by means of wire, radio, or television communication in interstate or foreign commerce."[4]

A wire fraud charge asserted in an insider trading case, unlike a securities fraud charge, would not require the DOJ to prove that the party disclosing the confidential information received a "personal" benefit or that the party receiving the information knew "that an insider breach[ed] a duty to the owner of the property.[5]

The wire fraud statute also can be utilized against schemes to defraud that take place largely outside the United States, as long as the scheme includes "conduct relevant to the statute's focus – that is, the use of the wires in furtherance of the schemes to defraud – occurring in the United States" as long as wires are "essential, rather than merely incidental, to [the] scheme to defraud."[6]

Implications

This case suggests that parties involved in digital assets may consider it wise to have robust protocols to detect and prevent "insider trading" similar to what has largely been adopted in the context of securities trading.

In addition, the case leaves open the question of whether a NFT is a security, but given the parallels in the government's description of the trading activity and alleged abuses to traditional securities fraud misappropriation cases, further regulation akin to what has been applied to cryptocurrencies (that are not Bitcoin or Ethereum-based cryptocurrencies) may be forthcoming.

We will be following this and other cases as appropriate.

Notes

[1] SEC Commissioner Hester Peirce has stated "Given the breadth of the NFT landscape, certain pieces of it might fall within our jurisdiction. People need to be thinking about potential places where NFTs might run into the securities regulatory regime."

[2] 15 U.S.C. Section 78j

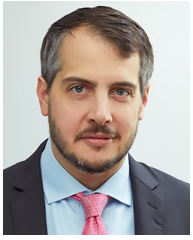
[3] Carpenter v. United States, 484 U.S. 19, 27 (1987)

[4] 18 U.S.C. Section 1343

[5] *United States v. Blaszczak*, 947 F. 3d 19, 36 (2d Cir. 2019). Also notable is that the "misappropriation" theory of insider trading typically arises when a defendant has purchased or sold a security on the basis of "material nonpublic information" obtained "in breach of a duty of trust or confidence" (*see* 17 CFR § 240.10b5-1). While it seems likely that the government will need to show that the information is valuable and confidential, it is unclear whether the government will be required to prove that the information allegedly used by Chastain was obtained in breach of any duty to OpenSea or that the information was "material" as conceptualized and understood under Section 10(b) of the Exchange Act.

[6] *United States v. Napout*, 963 F.3d 163, 180 (2d Cir. 2020)

About the authors


Mary Kuan (L), a partner at **Kleinberg, Kaplan, Wolff & Cohen PC**, advises clients on insider trading and other issues regarding trading, as well as regulatory filing obligations. She focuses on loan financings and other transactions involving extensions of credit, derivatives, bank debt and financial claims, and capital markets transactions. She represents clients regarding bespoke and exotic structured products, fixed-income and equity forwards, options, total return and credit default swaps and hedge fund-linked products and collateralized loan obligations. She can be reached at mkuan@kkwc.com. **Joshua K. Bromberg** (C), also a partner, represents individuals and companies in commercial and corporate litigation in state and federal courts, as well as before arbitration tribunals and regulatory agencies. In addition to crypto-related disputes, his advice extends to securities, contracts, employment, real property, trusts and estates, and intellectual property matters. He can be reached at jbromberg@kkwc.com. **Jared R. Gianatasio** (R), also a partner, advises clients on over-the-counter and exchange traded derivatives transactions and regulation, counterparty trading and brokerage relationships, and investment fund regulatory matters under U.S. commodities and securities laws. He represents both traditional private funds and crypto-native clients on digital asset-related issues. He can be reached at jgianatasio@kkwc.com. The authors are all based in New York. This article was originally published June 8, 2022, on the firm's website. Republished with permission

This article was published on Westlaw Today on June 22, 2022.