NOW & NEXT

Government Investigations & White Collar Alert

JUNE 21, 2022

DOJ charges "First Ever" digital asset insider trading scheme

By Mark D. Lytle, Daniel Schnapp, Colin T. Missett, and John Eden

The recently-unsealed OpenSea indictment is limited to alleged violations of the wire fraud and money laundering statutes; so how does the conduct alleged amount to "insider trading," as DOJ's press release states?

What's the Impact?

- By declining to charge securities fraud, DOJ appears to be avoiding creating any legal precedent regarding whether NFTs (or other digital tokens) are considered securities
- Everyone operating in the cryptocurrency space, including individuals and companies based overseas, should evaluate their compliance programs and insider trading policies
- This prosecution signals DOJ's belief that it has broad authority to prosecute operators in the digital asset space

On June 1, 2022, the U.S. Attorney for the Southern District of New York unsealed a two-count indictment of a former employee of Ozone Networks, Inc. (d/b/a OpenSea), Nathanial Chastain,

charging him with wire fraud and money laundering in connection with what the U.S. Department of Justice (DOJ) press release called "a scheme to commit insider trading in Non-Fungible Tokens [(NFTs)]."[1] The indictment alleges that in Mr. Chastain's role as a product manager at OpenSea, he selected the NFTs that would be featured on OpenSea's homepage, knew this information before members of the public, and knew that the values of NFTs featured on the homepage typically rose in value.[2] The government alleges that Mr. Chastain's insider trading scheme consisted of his misappropriation of this confidential business information "in violation of duties of trust and confidence he owed to his employer." Specifically, Mr. Chastain allegedly purchased certain NFTs before OpenSea began featuring them and then subsequently sold the same NFTs for a profit once OpenSea had posted them on the homepage, and their value had increased.

Notably, despite tracking language typically found in cases brought under Section 10(b) of the Securities Act of 1934, the indictment **does not** include a securities fraud count but, instead, only charges wire fraud and money laundering. Due to the absence of any allegation that the scheme involved a "security," the indictment does not actually allege "insider trading," as the U.S. Securities and Exchange Commission (SEC) defines it.[3]

Insider trading under the wire/mail fraud statutes

Although insider trading prosecutions in the modern era typically involve charges under Section 10(b) of the Securities Act of 1934, there is precedent for the stand-alone use of the wire and/or mail fraud statute to prosecute insider trading. Prior to the SEC's promulgation of Rule 10-b(5), for example, insider trading in securities had been prosecuted through the wire fraud statute alone.[4] Although modern indictments involving insider trading in securities typically contain counts for both securities fraud and wire and/or mail fraud in the same indictment,[5] the wire/mail fraud statutes also have been used by DOJ to prosecute instances of insider trading in financial products that are not securities, including commodities and commodities futures.[6]

When proceeding under the wire and/or mail fraud statutes in the absence of securities fraud counts, the government's burden is arguably easier under many fact patterns, as it need only establish two basic elements: (i) a scheme to defraud (i.e., to deprive another of money or property by means of false pretenses) and (ii) use of the mail or wires for purposes of executing

---

[1] Former Employee Of NFT Marketplace Charged In First Ever Digital Asset Insider Trading Scheme, U.S. DEPARTMENT OF JUSTICE (June 1, 2022).

[2] Indictment, *United States v. Nathanial Chastain*, No. 22-cr-305 (June 1, 2022).

[3] *See* Insider Trading, U.S. SECURITIES AND EXCHANGE COMMISSION.

[4] *See United States v. Groves*, 122 F.2d 87, 89 (2d Cir. 1941).

[5] *See* William K.S. Wang, Application of the Federal Mail and Wire Fraud Statutes to Criminal Liability for Stock Market Insider Trading and Tipping, 70 U. Miami L. Rev. 220, 226–27 & n.16 (2015) (collecting cases).

[6] *See id.* at n.133 (citing *United States v. Sleight*, 808 F.2d 1012, 1014 (3d Cir. 1987) (applying mail fraud to cocoa futures); *United States v. Dial*, 757 F.2d 163, 164 (7th Cir. 1985) (applying mail and wire fraud to silver futures)).

the scheme. 18 U.S.C. §§ 1341, 1343. The Supreme Court has interpreted the "property" aspect of the wire and mail fraud statutes broadly to include "intangible" property, including confidential business information.[7] If the government proceeds to trial in Mr. Chastain's case, then it will have the burden of establishing that Mr. Chastain's conduct deprived his employer of a property right analogous to those rights previously recognized by the Supreme Court.

The government's decision to proceed in the absence of a securities fraud count means that it need not establish the elements of securities fraud, including as relevant to many digital assets, that the conduct involved a "security" as defined by *SEC v. W.J. Howey Co.*[8] and its progeny. By declining to charge securities fraud in this case, DOJ thus necessarily avoids creating any legal precedent on the question of whether NFTs (or other digital tokens) are considered securities.

Critical implications for companies operating in the digital asset space

DOJ's indictment of Mr. Chastain comes at a time when Congress[9] and financial regulators are attempting to determine a framework for regulating digital assets and devoting resources to carry out their enforcement priorities in this space. DOJ's prosecution of an employee of a major market participant signals DOJ's belief that it already possesses the authority to prosecute alleged financial crime in the digital asset economy, including through use of the same statutes it routinely employs to prosecute traditional fraud in various other sectors of the economy. If the government ultimately achieves a conviction in this case—whether at trial or through a guilty plea—it will embolden DOJ to continue to charge actors and companies in the digital asset space under novel applications of routinely used statutes.

Moreover, given the breadth and reach of the wire fraud statute charged in this case, the indictment should serve as a wake-up call to all crypto market participants—including those abroad—that employee conduct and business practices once believed to be beyond the reach of prosecutors and regulators could be subject to scrutiny. Indeed, not only is the wire fraud statute broadly applicable to all types of fraud, but its jurisdictional reach could extend to schemes that largely take place outside of the United States so long as the "use of the wires in furtherance of the scheme to defraud . . . 'occurred in the United States,'" and that "'use of the wires . . . was 'essential, rather than merely incidental'" to the scheme to defraud.[10]

It is, therefore, incumbent on companies operating in the cryptocurrency space to evaluate the sufficiency of their compliance program, including their insider trading policy. Crypto companies should closely scrutinize business units that regularly maintain material non-public information to ensure that appropriate safeguards are in place for protecting that information. NFT platforms, in particular, should proactively evaluate how their offerings could be used to support, directly or

---

[7] *See Carpenter v. United States*, 484 U.S. 19, 25–26 (1987).

[8] *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).

[9] Lummis, Gillibrand Introduce Landmark Legislation To Create Regulatory Framework For Digital Assets (June 7, 2022).

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

indirectly, money laundering activities, and, whenever possible, those platforms should adopt technological and policy-based solutions to preempt such activities. Given the increasing potential that DOJ and other U.S.-based financial regulators will continue to explore the bounds of the statutes from which they derive their authority, digital asset companies should consider evaluating all of their business units to ensure they anticipate potential shifts in the regulatory landscape. If compliance issues are identified, early engagement with DOJ or other regulators through qualified counsel may be critical to a favorable corporate resolution.

Seek legal counsel

Nixon Peabody's Government Investigations and White Collar practice group advises companies and individuals that receive civil investigative demands, subpoenas, or any other requests for information from various federal and state agencies, including DOJ, the SEC, the Commodity Futures Trading Commission, the Financial Industry Regulatory Authority, and state attorney general offices. Nixon Peabody's Blockchain and Digital Assets team and Cybersecurity & Privacy team can further assist you in conducting business in this rapidly changing marketplace.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Mark D. Lytle
202.585.8435
mlytle@nixonpeabody.com

Daniel A. Schnapp
212.940.3026
dschnapp@nixonpeabody.com

Colin T. Missett
617.345.1029
cmissett@nixonpeabody.com

John Eden
415.984.8360
jeden@nixonpeabody.com