Client Alert: DOJ Charges Former NFT Marketplace Employee with Insider Trading

On June 1, 2022, the United States Attorney for the Southern District of New York unsealed a two-count indictment of Nathaniel Chastain, charging him with wire fraud and money laundering, and accusing him of "insider trading in non-fungible tokens [NFTs]" through an online digital asset marketplace operated by his employer, Ozone Networks, Inc. d/b/a OpenSea ("OpenSea").[1] The indictment is a watershed moment, marking the first time federal prosecutors have brought insider trading charges for alleged insider trading in digital assets. The wire fraud count, a somewhat non-conventional theory in an insider trading case, reveals that the Department of Justice is willing to prosecute what it views as insider trading, whether or not the asset being traded is considered a "security." Digital asset traders and those who operate platforms facilitating digital asset transactions should consider this prosecution a warning shot.

The government's indictment alleges an insider trading scheme pursuant to which Mr. Chastain: (i) misappropriated OpenSea's confidential business information regarding NFTs it planned to feature on its homepage; (ii) bought those NFTs through an anonymous account before OpenSea began featuring them; and (iii) then sold the NFTs for a sizable profit once OpenSea promoted them. Despite the government's reliance on the criminal wire fraud statute to bring its action, the wording of the allegations in the indictment – that Mr. Chastain acted "[i]n violation of the duties of trust and confidence . . . owed to his employer" and that he "exploited his advanced knowledge" to overcharge his counterparties for the digital artworks – is consistent with the language found in a typical insider trading case brought under the federal securities laws.

The charges against Mr. Chastain arrive in the context of a long running debate over whether and how laws designed to protect consumers and financial markets can be applied to digital assets such as cryptocurrencies and NFTs. Despite the assertion in August 2021 by SEC Chair Gary Gensler that this class of digital assets "is rife with fraud, scams, and abuse,"[2] the Commission has yet to offer any definitive rulemaking clearly defining what is, and is not, a security in this space. Instead, several years ago, the SEC staff offered "a framework for analyzing whether a digital asset has the characteristics of one particular type of security – and 'investment contract,'"[3] and since then, has continued to regulate by enforcement, leaving digital asset companies, patrons, and counsel to navigate an uncertain and constantly evolving landscape.[4]

Yesterday's unsealed indictment is significant because it sidesteps the knotty legal implications and fact-intensive analysis required under the securities laws as to whether a token is a security, by declining to charge Mr. Chastain with securities fraud. Traditionally, insider trading cases are charged

---

1 DOJ Press Release No. 22-180, "Former Employee Of NFT Marketplace Charged In First Ever Digital Asset Insider Trading Scheme," (June 1, 2022), *available at* https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-charged-first-ever-digital-asset-insider-trading-scheme; *see also* Indictment, *U.S. v. Chastain*, 22-cr-305, *available at* https://www.justice.gov/usao-sdny/press-release/file/1509701/download.

2 Gary Gensler, "Remarks Before the Aspen Security Forum," (Aug. 3, 2021), *available at* https://www.sec.gov/news/public-statement/gensler-aspen-security-forum-2021-08-03.

3 SEC Strategic Hub for Innovation and Financial Technology, "Framework for 'Investment Contract' Analysis of Digital Assets," *available at* https://www.sec.gov/files/dlt-framework.pdf.

4 For more on this piecemeal approach, please refer to our firm's earlier memorandum, "Review of 2021 Trends in SEC Crypto Enforcement Actions," (Feb. 3, 2022), *available at* https://www.quinnemanuel.com/the-firm/publications/review-of-2021-trends-in-sec-crypto-enforcement-actions/.

— either civilly or criminally — pursuant to a robust line of case law developed from Section 10(b) of the Securities Exchange Act of 1934 (the "Exchange Act"), which 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." 15 U.S.C. Section 78j. If the suspect traded does not involve the purchase or sale of *a security*, it cannot give rise to charges under the securities fraud statute.

By contrast, the DOJ has much greater leeway to bring fraud cases under the wire fraud statute, which "reach[es] any scheme to deprive another of money or property by means of false or fraudulent pretenses, representations, or promises," *Carpenter v. United States*, 484 U.S. 19, 27 (1987), as long as that scheme is carried out "by means of wire, radio, or television communication in interstate or foreign commerce," 18 U.S.C. § 1343 – *i.e.*, any telephonic, electronic, or digital communication that crosses state lines.[5] To obtain a conviction under Section 1343, the government need not prove: (i) that the victim of the fraud suffered economic loss; (ii) that the perpetrator of the fraud obtained a benefit; (iii) that the property subject to the scheme was tangible; (iv) that any misrepresentations or omissions conveyed in the course of the scheme meet the standard for materiality under Section 10(b) of the Exchange Act and related Supreme Court precedent;[6] or (v) that such misrepresentations and omissions actually were transmitted via "wire."[7] Indeed, this is not the first time that the DOJ has relied on the wire fraud statute to pursue insider trading "stretch cases" on theories that are not captured by the federal securities laws – and where the SEC could not necessarily act. In *United States v. Blaszczak*, for example, the DOJ obtained a conviction for insider trading activity based on the misappropriation of a government agency's confidential nonpublic information, without having to prove two of the necessary elements under Section 10(b) of the Exchange Act and Rule 10b-5: (i) that the party disclosing the information received a "personal benefit"; and (ii) that the party receiving the information knew "that an insider breach[ed] a duty to the owner of the property." 947 F.3d 19, 36 (2d Cir. 2019).

The government's willingness to pursue insider trading cases using the theory advanced in the Chastain indictment also has significant implications for digital asset platforms and their patrons that operate outside the United States. Unlike the securities fraud statute, the wire fraud statute can be enforced against schemes to defraud that took 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," and as long as the "use of the ... wires" was "essential, rather than merely incidental, to [the] scheme to defraud." *United States v. Napout*, 963 F.3d 163, 180 (2d Cir. 2020) (internal quotation marks omitted). This extraterritorial test is far less onerous for the government than the one it must meet under *Morrison* to charge Section 10(b) for transactions outside the United States. *See Morrison v. Nat'l Australia Bank Ltd.*, 61 U.S. 247, 267 (2010) ("[I]t is . . . only transactions in securities listed on domestic exchanges, and domestic transactions in

---

[5] This includes schemes carried out over the internet, either where one user sends a signal across state lines to contact a host server, or "where computers in multiple states access the same website." *U.S. v. Kieffer*, 681 F.3d 1143, 1155 (10th Cir. 2012).

[6] *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, 280 (2015) ("There is no assurance that the mail fraud statute will be applied in a fashion consistent with Rule 10b-5.").

[7] *See United States v. Jinian,* 725 F.3d 954, 960 (9th Cir. 2013) (wire can form the basis of a wire fraud conviction even if it did not involve a fraudulent communication; need only further the scheme to defraud.

other securities, to which § 10(b) applies."). Charges for conspiracy, as well as aiding and abetting, may also be easier to prove with respect to digital asset transactions under the wire fraud statute.

The unsealed indictment in *U.S. v. Chastain* could represent a meaningful expansion of regulation and enforcement actions applicable to a wide range of digital assets that might otherwise lie beyond the grasp of the SEC. In the wake of this prosecution, digital asset platforms and firms that invest in digital assets may wish to re-evaluate their compliance and insider trading policies as well as any at risk business practices.

* * *

If you have any questions about the issues addressed in this memorandum, or if you would like a copy of any of the materials mentioned in it, please do not hesitate to reach out to:

Michael Liftik
Co-Chair, SEC Enforcement Practice
Email: michaelliftik@quinnemanuel.com

David M. Grable
Co-Chair, National Trial Practice
Email: davegrable@quinnemanuel.com
Phone: 213-443-3669

Sarah Heaton Concannon
Co-Chair, SEC Enforcement Practice
Email: sarahconcannon@quinnemanuel.com
Phone: 202-538-8122

Stacylyn Doore
Email: stacylyndoore@quinnemanuel.com
Phone: 617-712-7121

Kurt Wolfe
Email: kurtwolfe@quinnemanuel.com
Phone: 202-538-8379

Alex Zuckerman
Email: alexzuckerman@quinnemanuel.com
Phone: 212-849-7000

To view more memoranda, please visit www.quinnemanuel.com/the-firm/publications/
To update information or unsubscribe, please email updates@quinnemanuel.com