Professional Perspective

Application of Wire Fraud Statute to Digital Asset Insider Trading

Contributed by Joshua Robbins, Buchalter

Bloomberg Law

Application of Wire Fraud Statute to Digital Asset Insider Trading

Contributed by Joshua Robbins, Buchalter

The dark side of digital assets—cryptocurrency, non-fungible tokens (NFTs), and other blockchain-based financial innovations—is no secret. Reports of theft, money laundering, and various scams involving the technology circulate daily, to the point that even its supporters encourage law enforcement to crack down on the worst practices.

The Department of Justice (DOJ), along with other agencies, has responded, pursuing criminal charges against a variety of alleged offenses. But until recently, despite much discussion of the issue, that did not include prosecution of insider trading in digital assets.

That changed on June 1, 2022, when the US Attorney's Office for the Southern District of New York unsealed a grand jury indictment against Nathaniel Chastain, a former product manager at online NFT marketplace OpenSea. The government alleges that Chastain used his advance knowledge of which NFTs the company would feature on its web page to profitably trade on those items, and it has touted the case as the first prosecution of digital asset insider trading.

Notably, the indictment does not charge Chastain under the laws typically used to prosecute insider trading. Likely because it is not clear whether NFTs are "securities" or "commodities" covered by those laws, the government has instead used the federal wire fraud statute, a broad anti-fraud law used to charge various white-collar offenses.

While there is solid historical precedent for using the wire fraud statute to charge insider trading, there may also be reason to question the viability of that approach. The Supreme Court has acted forcefully to rein in DOJ's expansive use of the law, most recently and strikingly in *Kelly v. United States*, 140 S. Ct 1565 (2020), and then in the insider trading case *Blaszczak v. United States*, 141 S. Ct 1040 (2021). The court's reasoning in *Kelly* poses at least a potential challenge to insider trading prosecutions based on wire or mail fraud theories—and thus to DOJ's apparent strategy for combating insider trading in novel digital assets.

Increased Concern Over Insider Trading

Concern over insider trading in cryptocurrency and other digital assets has been rising for some time. In December 2017, for example, leading crypto exchange Coinbase halted transactions in Bitcoin Cash after suspicions arose that its employees had purchased the coins in advance of an announcement that they would be added to the Coinbase platform.

The allegations against Chastain further illustrate the potential for abuse in this area. His former employer OpenSea operates the largest online platform for buying and selling NFTs, which have been analogized to digital certificates of ownership for digital artwork or other items. The price of NFTs can change dramatically, and NFTs that are featured on OpenSea's main web page—and thus gain high visibility among its users—often increase rapidly. For that reason, OpenSea keeps confidential advance information about which NFTs will be shown on the page.

According to the recent indictment, Chastain's job at OpenSea included choosing the NFTs to be featured on the home page. He thus had early, non-public knowledge of the identify of those NFTs. Allegedly, Chastain used that information to purchase dozens of the NFTs before they were featured, and then to sell them at prices from two to five times higher after they were posted. OpenSea later fired Chastain and publicly confirmed that the trading had occurred.

In a sense, what Chastain is accused of doing is indistinguishable from classic insider trading: using non-public information from one's employer, without permission, to gain advantage in trading in assets linked to that employer. The novelty is mainly in the type of asset being traded: digital tokens on a blockchain, rather than stocks or options listed on a securities exchange.

Traditional Tools May Not Work

Historically, DOJ charged insider trading cases under Section 10(b) of the Securities Exchange Act of 1934, 15 U.S.C. §78j. Although Section 10(b) does not actually mention insider trading, a long series of decisions from the Supreme Court and other courts have established that a company insider who trades on the company's confidential information can violate the statute. In 2002, Congress added a new criminal securities fraud statute at 18 U.S.C. § 1348, in part to simplify DOJ's pursuit of securities-related fraud.

Neither of those laws, however, is well-suited to prosecution of insider trading in digital assets such as NFTs. As the name of the Securities Exchange Act implies, that statute is aimed at trading in "securities," and Section 10(b) expressly covers only fraud "in connection with the purchase or sale of a security" or a "securities-based swap agreement." Section 1348, meanwhile, covers fraud in connection with securities, commodities, or commodities-based options.

There is currently no consensus as to which digital assets qualify as securities or commodities. The most widely cited test for defining a "security" comes from the 1946 Supreme Court decision in *S.E.C. v. W.J. Howey Co.*, 328 U.S. 293 (1946), and turns on whether "a person invests his money in a common enterprise and is led to expect profits solely from the effects of the promoter or third party."

While the Securities and Exchange Commission (SEC) has issued a "Framework" for applying the *Howey* test to digital assets, it consists of multiple factors and the agency has taken a case-by-case approach to which digital assets would qualify. The crypto industry has often vigorously pushed back against the SEC's approach. So far, relatively few courts have weighed in on the issue, and those that have treat it as highly dependent on the specific design of the asset itself. See, e.g., *Bibox Group Holdings Limited Securities Litigation*, 534 F. Supp. 3d 326, 336 (S.D.N.Y. 2021).

The Commodity Futures Trading Commission (CFTC), meanwhile, has taken the position that cryptocurrencies do qualify as "commodities" under the Commodity Exchange Act but has not yet said the same about NFTs. While a number of district courts have agreed with the CFTC as to cryptocurrency, there have been no appellate decisions on point. See, e.g., *CFTC v. McDonnell*, 287 F. Supp. 3d 213 (E.D.N.Y. 2018). The Responsible Financial Innovation Act recently proposed in the US Senate would legislatively define most digital assets as commodities, though its passage and final language remain uncertain.

Criminal prosecution is a poor vehicle for resolving the debate. As the Supreme Court has explained, "ordinary notions of fair play" and "due process" require that criminal laws clearly provide "fair warning" as to exactly what conduct is illegal. The Rule of Lenity, a principle of statutory interpretation under which ambiguous criminal laws are construed in favor of the defendant, was developed to effectuate these principles and courts have repeatedly invoked it to preclude prosecution when key statutory terms are unclear.

In *Yates v. United States,* 574 U.S. 528 (2015), for example, the Supreme Court applied the lenity doctrine to hold that a fish that a federal agent asked the defendant to retain as evidence following an investigation was not the type of "tangible object" whose concealment would violate an obstruction of justice statute. To threaten criminal conviction and imprisonment for securities fraud involving items it is has never been clear are securities at all would hardly seem more appropriate.

Wire & Mail Fraud Statutes as Alternatives

Perhaps for the above reasons, DOJ did not indict Chastain under either the Exchange Act or § 1348. Instead, it charged him with wire fraud under 18 U.S.C. § 1343, alleging that he had "misappropriated OpenSea's confidential business information" in violation of his duties to the company. This approach to charging insider trading is hardly unprecedented. Indeed, its pedigree includes a unanimous Supreme Court decision, *Carpenter v. United States*, 484 U.S. 19 (1987), but recent reconsideration of the wire fraud statute may cast new doubt on it.

Intuitively, wire or mail fraud and insider trading make for an awkward fit. Violation of § 1343 requires a "scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises." Courts have generally held that it entails outright deception. For example, the Ninth Circuit requires that the defendant have acted with intent to "deceive and cheat" a victim. *United States v. Miller*, 953 F.3d 1095 (9th Cir. 2020).

Insider trading, however, does not typically require deception as commonly understood. The putative victim—the company whose confidential information is misused—is usually not told anything about the disclosure or trading itself.

The Supreme Court nonetheless blessed wire fraud charges for insider trading in *Carpenter*. In that case, a Wall Street Journal columnist leaked valuable information on pre-publication articles to brokers who used the tips to trade in stocks. DOJ charged him with wire fraud, and the court rejected without dissent the defendant's argument that the conduct did not meet the elements of the statute.

As the court explained, confidential business information is property "to be gathered at the cost of enterprise, organization, skill, labor, and money, and to be distributed and sold to those who will pay money for it." It found that the defendant in that case had defrauded the newspaper of exclusive control over that information by promising to protect it and then secretly violating that promise.

Both before and after *Carpenter,* DOJ used the wire and mail fraud statutes in a number of insider trading cases, although they later fell out of favor. In response to other court decisions restricting certain types of insider trading charges under the Exchange Act, some commentators suggested that the practice could be revived as a solution. The Chastain indictment suggests that DOJ views the wire fraud approach as a solution to the uncertainty as to whether the securities fraud laws apply to novel digital assets.

Limits on the Wire Fraud Statute

Carpenter, however, was not the Supreme Court's final word on wire fraud. In *Kelly*, the court considered whether state government officials had committed wire fraud when they used public funds to pay government staff to alter traffic patterns on a crowded bridge in order to create a traffic jam, as part of a scheme to punish a political rival. While the court acknowledged that the defendants had misappropriated valuable resources to engage in the scheme, it held that this did not amount to wire fraud under § 1343.

The court's reasoning in *Kelly* is important. Quoting its earlier decision in *McNally v. United States*, 483 U.S. 350, 358, the Court noted that "the wire fraud statute … prohibits only deceptive schemes to deprive the victim of money or property." It also said that the government had to show that "property" was an "object" of the fraud. That is, the "deceit" involved in the fraud must have had as its "object" the obtaining of the victim's money or property.

The court rejected the government's arguments that the defendants had defrauded the government of the bridge lanes themselves, and the relevant public employees' time and labor. As to the former, the court pointed out that that the defendants had not actually deprived the government of ownership of the lanes themselves. As to the latter, the court said that the misappropriation of the employees and their salaries was not actually the object of the scheme—it was not the employee labor the defendants were ultimately seeking—but rather an "incidental byproduct" of the effort to reach the real goal: political payback.

Kelly had an immediate impact on at least one type of insider trading prosecution. In *Blaszczak,* a former employee of the Centers for Medicare and Medicaid Services (CMS) was convicted of wire fraud after he obtained confidential information from a current CMS employee about future CMS rule changes, then passed the information to a hedge fund that traded on it. Following its decision in *Kelly*, the Supreme Court vacated and remanded *Blaszczak* to the Second Circuit to decide whether the conviction could stand.

When the case returned to the Second Circuit, DOJ conceded that under *Kelly*, Blaszczak's insider trading could not be charged as wire fraud and the conviction should be dismissed. As the government's brief explained, although the non-public information taken from CMS had economic value because the agency "invests time and resources into generating and maintaining the confidentiality of" the information, the deprivation of those things was not "an object of the fraud." Thus, the government said, the insider trading could not be wire fraud under *Kelly*.

Restrictions Could Reduce DOJ's Options

Although both *Kelly* and *Blaszczak* specifically concerned theft of government resources, their reasoning could extend to insider trading cases involving confidential private information, such as the planned NFT website content in Chastain's case. First, in insider trading cases, as in *Kelly,* the victim organization is not actually deprived of the information at issue. While it does lose exclusive control and use of that information, that was also true of the state government's temporary loss of control over the bridge lanes in *Kelly*.

Second, and more importantly, the misappropriation of confidential information is arguably never the "object" of an insider scheme, but merely a means to the ultimate end: profitable trading without risk. The Chastain indictment, for example, presumes that he exploited his advance, non-public knowledge of the OpenSea website features not because he sought that information for its own sake, but instead used it to ensure that he could purchase NFTs that would predictably go up in value. Under the logic of *Kelly*, as applied by DOJ in *Blaszczak*, that could allow Chastain to argue that his misuse of the information was only a "byproduct" of the scheme, and the wire fraud statute would not apply.

This argument is hardly unassailable, and at least one court has rejected something similar to it. In *United States v. Ramsey*, 19-CR-268 (E.D.PA Sept. 17, 2021), DOJ charged a defendant under § 1348 for a scheme involving insider trading in stock options. The defendant argued that § 1348 was modeled on the mail and wire fraud statutes, and the "object" of an insider trading scheme is not the deprivation of property (confidential information) from the victim. In dicta, the court disagreed and found that misappropriation of the information *was* an object of the scheme, making the case more comparable to *Carpenter* than to *Kelly*.

While the *Ramsey* court did not discuss *Blaszczak*, it may not be alone in finding *Kelly* inapplicable to typical insider trading. The *Kelly* decision did not discuss *Carpenter,* and courts may be hesitant to infer that it overruled the *Carpenter*'s approval of wire fraud charges for insider trading. Others may seek to narrow *Kelly* and *Blaszczak* by arguing that the cases really only concern government corruption, rather than private misconduct.

Conclusion

Even if the *Kelly/Blaszczak* reasoning is applied to insider trading in private information, and the wire and mail fraud statutes are no longer available in such cases, DOJ is not without potential options in digital assets cases. As discussed above, there is support for the position that many cryptocurrencies—if not NFTs—are "commodities," and thus insider trading in crypto may be covered by 18 U.S.C. § 1348, although that statute may present its own complications.

If courts or Congress solidify the notion that digital assets are "securities," DOJ may have a stronger basis for charging under either § 1348 or the Exchange Act—although it may remain risky in the case of NFTs and new forms of assets. But in the meantime, DOJ's effort to combat insider trading in this space will continue to face questions and legal challenges from defendants. As with regulation of digital assets in general, much remains to be seen.