Expect indictments in the NFT space soon

By Ian McGinley, Esq., Akin Gump Strauss Hauer & Feld LLP

FEBRUARY 4, 2022

Over the last few years, we have observed an uptick of federal criminal cases in the cryptocurrency space. These cases follow the massive flow of capital into this relatively new and rapidly developing market. For example, in 2017, an estimated $4.9 billion was raised through initial coin offerings ("ICOs") alone.

However, another sector involving digital assets is growing at an even faster pace — the Non-Fungible Token ("NFT") market. According to some estimates, trading in NFTs reached $22 billion in 2021, compared with $100 million in 2020. The Department of Justice has yet to bring a criminal case involving NFT markets, but that will change.

Cryptocurrency-related crimes have been designated a priority by Deputy Attorney General Lisa Monaco, who has established a National Cryptocurrency Enforcement Team ("NCET") that consists of a team of dedicated prosecutors who focus on a wide array of crimes, including NFT fraud. In the wake of reports about insider trading in NFT marketplaces, manipulation of NFT prices, and NFT creators embezzling funds, the DOJ is likely already looking for opportunities to bring prosecutions in this area.

What is an NFT, and where are they sold?

In general terms, NFTs represent unique digital assets, which are typically bought and sold using cryptocurrency. The transfer of ownership of NFTs is recorded on a blockchain, a digital ledger. NFTs are "non-fungible," unlike cryptocurrencies such as Bitcoin and Ethereum that can be swapped interchangeably.

Almost any unique asset can be an NFT, although NFTs have probably gained the most popularity in the form of virtual collectibles, like digital art and virtual trading cards. Some NFTs have sold for huge sums. In March 2021, the digital artist Beeple sold an NFT digital collage for $69 million. Twitter founder Jack Dorsey's first ever tweet sold for approximately $2.9 million as an NFT.

NFTs are generally sold on online marketplaces. One of the largest NFT marketplaces lists over 80 million NFTs. When a new NFT is listed on a marketplace, it's called a "drop," which often garners a lot of attention in the community, similar to an IPO.

Types of criminal cases we are likely to see going forward

In any industry growing as rapidly as the NFT space, and with little to no new rules specifically targeted to the industry, there will always be bad actors and fraud. Indeed, we have already seen reports about various types of potential fraud in these marketplaces. Below, I summarize these reports and offer some thoughts on cases that the DOJ may bring soon.

Insider trading. In September 2021, a senior employee at one of the largest NFT marketplaces was accused of buying NFTs right before the NFTs were dropped on the marketplace's front page, and then selling the NFTs after their price jumped. The employee made about $67,000. The marketplace later implemented new policies to prevent team members from using confidential information to purchase or sell any NFTs.

In the wake of reports about insider trading in NFT marketplaces, manipulation of NFT prices, and NFT creators embezzling funds, the DOJ is likely already looking for opportunities to bring prosecutions in this area.

Reports such as this suggest insider trading may be happening on NFT marketplaces, but is that a crime? The answer is arguably yes, although there are some legal nuances. For example, it is unclear whether a digital asset like an NFT is considered a "security" and therefore prosecutable under the criminal securities fraud statutes prohibiting insider trading. Under the Supreme Court's test in *United States v. Howey*, 328 U.S. 293 (1946), a security includes: (1) an investment of money; (2) in a common enterprise; (3) with a reasonable expectation of profit; and (4) to be derived from the efforts of others.

Under this standard, a simple NFT like a digital file exchanged between two parties on an exchange is unlikely to be considered a security — but there are certain NFT arrangements that might qualify. Consider a fractional arrangement, where an investor would share with others a partial interest in an NFT managed by the NFT creator — similar to owning shares of a stock. The shares could entitle their owners to profits from future sales of the NFT. In this scenario, the DOJ or Securities and Exchange Commission could seek to argue that the NFT should be considered a "security" and seek to bring insider trading charges under the federal securities laws.

But even if an NFT is not considered a security, insider trading in NFTs by marketplace employees could potentially constitute the crime of wire fraud. The wire fraud statute is broad, covering intentional schemes to defraud others using electronic communications, regardless of whether the conduct involves the purchase or sale of a security. In a different context, the Supreme Court found in the seminal insider trading case of *Carpenter v. United States*, 484 U.S. 19 (1987), that an employee who steals confidential information from his employer for personal profit is guilty of wire fraud.

The same principle likely applies here. In a potential wire fraud case, prosecutors could seek to charge NFT marketplace insiders with misappropriating confidential information obtained from their employers or other parties to whom they owe duties for their own personal profit. This would also not be entirely unprecedented — there have been prior cases where prosecutors have used the wire fraud statute to charge insider trading in instruments other than securities. For example, in *United States v. Dial*, 757 F.2d 163 (7th Cir. 1985), a federal appellate court upheld a futures broker's wire fraud conviction for insider trading in breach of his fiduciary duties to his customers. The DOJ prosecuted this case as wire fraud because the charges were filed before the Commodity Exchange Act was amended to include provisions prohibiting insider trading in the futures markets.

In any industry growing as rapidly as the NFT space, and with little to no new rules specifically targeted to the industry, there will always be bad actors and fraud.

Market manipulation. Another issue in NFT marketplaces, where buyers and sellers can remain anonymous, is the manipulation of NFT prices. This is commonly achieved through what is known as "wash trading," in which a person buys and sells the same NFT to create an appearance of market demand.

This is not a hypothetical concern. In October 2021, a white-haired, green-eyed pixelated character called CryptoPunk #9998 sold for half a billion dollars. Or so it seemed. As it turned out, the buyer and seller were the same person, who then turned around and tried to sell the same NFT for over a billion dollars. Perhaps this was a publicity stunt, but it underscores the potential for wash trading.

If an NFT is considered a security, wash trading could lead to securities fraud charges. Wash trading in NFTs is also arguably illegal under the wire fraud statute as a "scheme to defraud," in which the people doing the wash trading are, in effect, misrepresenting the artificially high price of the NFT to the would-be purchaser. In deciding whether to bring such a charge, prosecutors would likely focus on whether the perpetrator of the wash trade was acting with manipulative or fraudulent intent.

Rug pulls. A "rug pull" is essentially a take-the-money-and-run scheme in the cryptocurrency space. With respect to digital coins, a rug pull occurs when the developers of a new coin offer the coin for sale, in exchange for more established coins, such as Ethereum, for example.

After the new coin gains popularity and increases in value, the creators of the coin quickly cash out their Ethereum, draining the liquidity pool from the exchange and making the new coin worthless. This occurred in November 2021, when a cryptocurrency based on the blockbuster drama series Squid Games plummeted from $2,861 to $0, when the creators cashed out and disappeared.

Reports of similar types of rug pulls are also occurring in NFT markets. For example, in October 2021, it was reported that the creator of the Evolved Apes NFT vanished with $2.7 million in NFT sales. These particular NFTs were supposed to be used for a virtual fighting game. However, before the game was developed, the creator disappeared from the internet.

A rug pull is a quintessential scheme to defraud that can be prosecuted under the wire fraud statute. The challenge for prosecutors in bringing rug pull cases will be in identifying the bad actors, who typically hide their true identities on the NFT marketplaces and transfer their stolen proceeds through cryptocurrency wallets, outside of the banking system.

Money laundering. Finally, there is a general concern about money laundering. It's not difficult to see how NFT markets could be used by bad actors to disguise illegal proceeds by moving them through trade transactions to make the proceeds look legitimate, a practice known as trade-based money laundering. For example, imagine that John wants to launder $5 million in illegal proceeds to Jack. Jack could create an NFT, list it for $5 million, and accept the $5 million from John. Now the $5 million appears as representing the market value of the NFT.

In more traditional markets, the authorities can uncover this method of money laundering by comparing the value of the transaction against pricing histories for the goods in question. In a new and rapidly changing market like the NFT market, such a comparison is more difficult and subjective.

In addition, the U.S. Department of Treasury has not issued any regulations specific to NFT markets or indicated whether NFT market participants are subject to anti-money laundering requirements -- such as know your customer due diligence and filing suspicious activity reports.

For all these reasons, it is likely that institutions in the NFT space will attract additional regulatory scrutiny related to anti-money laundering practices from criminal and civil authorities.

Conclusion

As we saw in the wake of the ICO boom of 2017, criminal enforcement generally follows when an industry grows so rapidly, although there is usually a lag until prosecutions begin, after prosecutors learn the subject matter and investigate. The Department of Justice recently indicated its priority in targeting the cryptocurrency space by creating the NCET, which has a broad mandate to pursue prosecutions involving the misuse of cryptocurrency to commit crime. Given this focus by DOJ and reports of fraud in NFT marketplaces, we should expect to see cases in the NFT space soon.

About the author

Ian McGinley is a partner in **Akin Gump Strauss Hauer & Feld**'s white collar defense group in New York. Before joining the firm, he served as a prosecutor in the Southern District of New York, where he was Co-Chief of the Complex Frauds and Cybercrime Unit, and a member of the Securities and Commodities Fraud Task Force. He can be reached at imcginley@akingump.com.

This article was first published on Reuters Legal News and Westlaw Today on February 4, 2022.