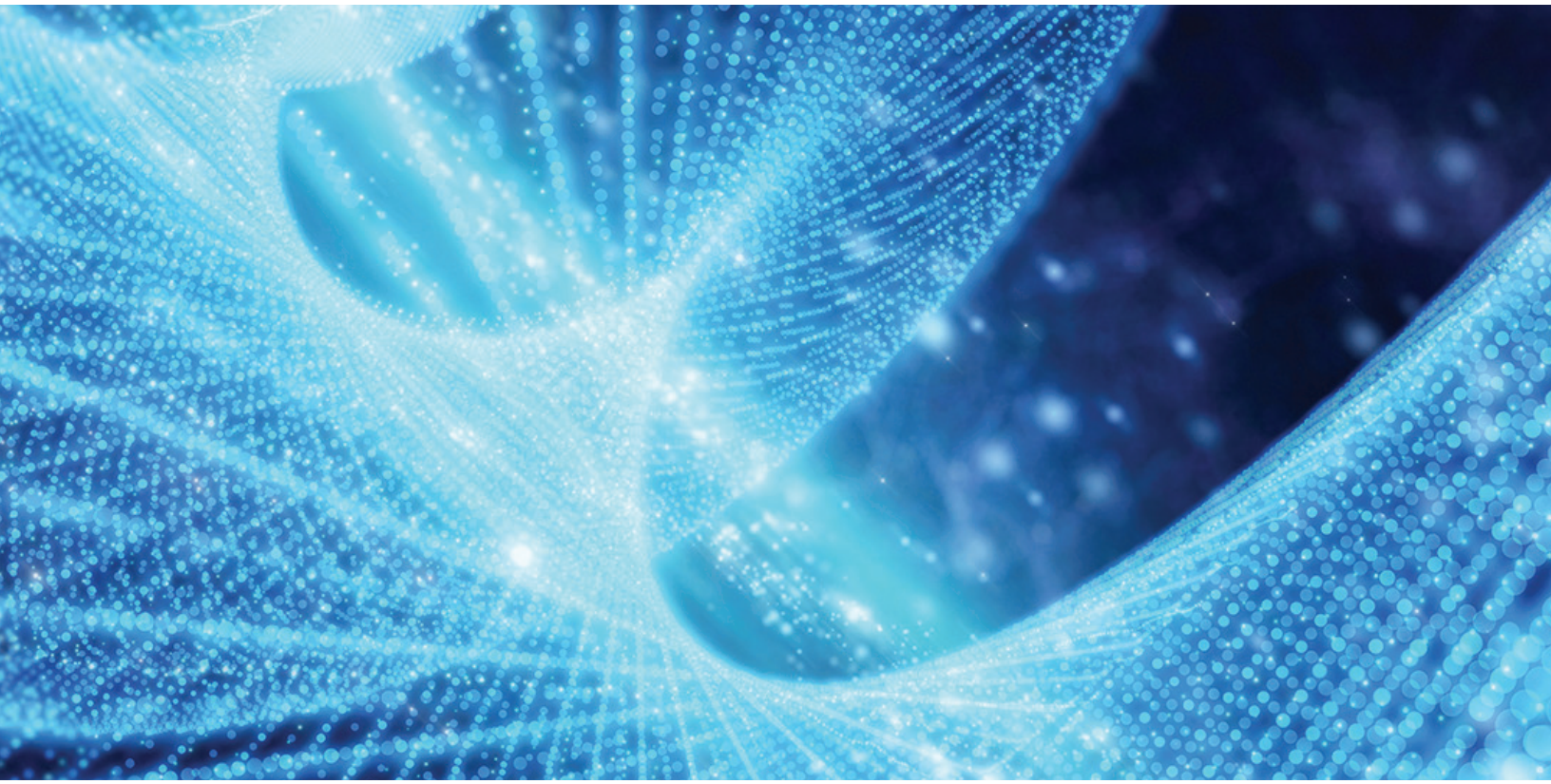
BakerHostetler

Introduction to Non-Fungible Tokens – Part 6

Combatting Fraud and Corruption in the NFT Market



AUTHORS

George A. Stamboulidis
gstamboulidis@bakerlaw.com

Christina O. Gotsis
cgotsis@bakerlaw.com

Jordan R. Silversmith
jsilversmith@bakerlaw.com

Robert A. Musiala Jr.
rmusiala@bakerlaw.com

On Oct. 6, 2021, the U.S. Department of Justice (DOJ) announced the creation of a National Cryptocurrency Enforcement Team to tackle investigations and prosecutions of criminal misuses of cryptocurrency.[1] As the non-fungible token (NFT) market continues to expand, DOJ's heightened focus on cryptocurrency has begun to encompass NFTs. Just as with any other market, a particular focus of DOJ's efforts will be to identify and prosecute fraud. At the same time, fraudulent activity is becoming increasingly common in the NFT market.[2] This paper provides an overview of common fraud typologies in the NFT market and steps NFT market actors can take to protect themselves from becoming victims of fraud or unwittingly facilitating fraud.

1 Press Release, "Deputy Attorney General Lisa O. Monaco Announces New Cryptocurrency Enforcement Team," Dept. of Just., Oct. 6, 2021, available at https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team.

2 *The Chainalysis 2021 NFT Market Report*, https://go.chainalysis.com/nft-market-report.html.

Recent Examples of Fraudulent Activity in the NFT Market

The following recent examples show some of the NFT fraud typologies that have arisen to date:

- In August 2021, a fake Banksy NFT was sold for £244,000 on a now-deleted page on the artist's website following a hack. After wide press coverage, the hacker eventually returned most of the money to the buyer.[3]In September 2021, insider trading allegations shook the NFT space after leading NFT marketplace OpenSea confirmed reports that an employee purchased NFTs they knew were to be featured on the company's front page before they appeared publicly only to resell them at a higher valuation after the NFTs were featured on OpenSea's site.[4]
- On Jan. 10, NFT marketplace LooksRare launched as a competitor to OpenSea, attracting high volumes with its token incentives and trading rewards; however, on Jan. 30, Cointelegraph reported that a very small group of traders executing trades worth hundreds of thousands of dollars between their own wallets reaped most of the trading rewards.[5]
- On Jan. 15, NFT artist Liam "Sharpy" Sharp announced that he would be shutting down his DeviantArt gallery due to piracy of his NFTs and the cumbersome process artists must undertake to report every instance of piracy to the NFT platform.[6]
- Between Jan. 23 and 27, a series of blockchain transactions show that cryptocurrency used to purchase an NFT of Melania Trump's first official state visit came from a wallet that belongs to the entity that originally listed the project for sale.[7]
- On Jan. 24, Elliptic identified at least five attackers who exploited still-active old marketplace ads to purchase $1.1 million in NFTs from OpenSea users – well below market value – later selling them for multiples of the purchase price. At least one of the attackers sent his profits through a mixing service.[8]
- On Jan. 27, VICE reported that some NFTs on OpenSea were utilizing custom code to capture viewers' IP addresses, potentially for the purpose of mining other identifiable information of the viewers.[9]
- On Feb. 2, Chainalysis published a study reporting NFT wash traders made nearly $8.9 million in profits, likely from sales to unsuspecting buyers who believed the NFT they bought had grown in value. The study also reported that $2.4. million from illicit addresses were sent to NFT marketplaces for money laundering purposes, including significant amounts of stolen funds – even those with sanctions risk.[10]
- On Feb. 11, NFT marketplace Cent announced it was suspending sales of NFTs due to rampant NFT fakes and plagiarism and may introduce centralized controls as a short-term measure to reopen the marketplace.[11]
- On Feb. 14, HM Revenue & Customs of the British government seized its first NFTs as possible proceeds of money-laundering methods in a suspected £1.4 billion value-added tax (VAT) fraud in which two individuals tried to claim back more VAT than they were owed using stolen identities, unregistered phones and false invoices to hide their identities.[12]
- On Feb. 19, OpenSea announced it was investigating a potential phishing campaign that took advantage of its planned smart contract upgrade to steal NFTs of at least 17 NFT holders.[13]
- On March 24, DOJ charged two defendants in connection with the execution of a $1 million NFT "rug pull" scheme. The defendants created and sold NFTs before abruptly abandoning the project, shutting down the website and making off with investors' money just hours after the NFTs sold out.[14]
- On April 25, Cointelegraph reported that Yuga Labs, developer of the Bored Ape Yacht Club NFTs, fell victim to hackers who breached its social media account and shared phishing scam links to a website that was used to steal NFTs from users who

3 "Fake Banksy NFT sold through artist's website for £244k," Aug. 31, 2021, available at https://www.bbc.com/news/technology-58399338.

4 "Largest NFT marketplace admits the fix was in, surprising no one," Dec. 11, 2021, available at https://sea.mashable.com/tech/17544/largest-nft-marketplace-admits-the-fix-was-in-surprising-no-one.

5 https://cointelegraph.com/news/clever-nft-traders-exploit-crypto-s-unregulated-landscape-by-wash-trading-on-looksrare.

6 https://www.rediff.com/business/report/is-the-nft-youre-buying-authentic/20220115.htm.

7 https://www.msn.com/en-us/money/markets/money-that-won-melania-trump-nft-came-from-melania-trump-wallet/ar-AATWIKv.

8 https://www.elliptic.co/blog/bug-allows-nfts-worth-over-1-million-to-be-stolen.

9 https://www.vice.com/en/article/xgdvaz/nft-steal-ip-address-opensea.

10 https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-nft-wash-trading-money-laundering/.

11 https://www.reuters.com/business/finance/nft-marketplace-shuts-citing-rampant-fakes-plagiarism-problem-2022-02-11/.

12 https://www.nbcnews.com/tech/tech-news/british-authorities-just-seized-nfts-first-time-14-million-fraud-probe-rcna16109.

13 https://www.coindesk.com/business/2022/02/20/opensea-investigating-exploit-rumors-as-users-complain-of-missing-nfts/; https://www.coindesk.com/business/2022/02/21/opensea-says-phishing-attack-impacted-17-users/.

14 https://www.justice.gov/usao-sdny/pr/two-defendants-charged-non-fungible-token-nft-fraud-and-money-laundering-scheme-0.

connected their MetaMask wallets to the website. Approximately 100 NFTs, with an estimated value of more than $40 million, were stolen during the attack.[15]

- On April 28, the Joint Chiefs of Global Tax Enforcement (J5), an intergovernmental organization dedicated to combating transactional tax crime, issued an intelligence bulletin entitled "J5 NFT Marketplace Red Flag Indicators" that provides guidance on NFT fraud indicators and how to improve fraud detection in the NFT market.[16]
- On May 11, securities regulators in five states filed enforcement actions against Flamingo Casino Club, a metaverse casino with alleged ties to Russia, ordering the casino to halt the sale of its NFTs. Among other things, the regulators alleged that Flamingo Casino Club sold unregistered "securitized NFTs," purportedly giving would-be investors a portion of the casino's profits; used fake information to conceal the identities of its principals; and falsely claimed to have partnerships with and endorsements from various high-profile businesses, including a brick-and-mortar casino in Las Vegas.[17]
- On June 1, DOJ published a press release announcing the unsealing of an indictment charging a former OpenSea employee with wire fraud and money laundering "in connection with a scheme to commit insider trading." The indictment relates to reports confirmed by OpenSea in September 2021 and alleges that the former employee used confidential information to purchase NFTs with the knowledge that the NFTs would be featured in the future on the NFT marketplace's homepage, at which time the NFT value would likely increase and the former employee would gain a personal financial benefit.[18]
- On June 4, CoinDesk reported that Yuga Labs suffered a hack of its social media server, with hackers stealing NFTs valued at approximately $360,000 via a phishing scam posted on the social media channel.[19]
- On June 30, DOJ announced criminal charges against a defendant who allegedly orchestrated an NFT rug-pull scheme by abruptly ending a purported NFT investment project, deleting its website and absconding with investors' money. The defendant and his coconspirators allegedly then laundered $2.6 million of investors' funds through "chain hopping," a form of money laundering in which one type of coin is converted to another and funds are moved across multiple cryptocurrency blockchains.[20]

Counterfeit NFTs

1. Common Typologies

The value of an NFT is generally derived from the underlying media (NFT Media) and the associated artist, rarity and authenticity.[21] The NFT authenticates the NFT Media, in many respects, by proving that the NFT Media was attached to the NFT by a specific person at a specific point in time. However, the NFT Media cannot authenticate the NFT, and as recent reports have described,[22] there appears to be a growing problem where counterfeiters download an image of an artist's work and use it to mint and sell NFTs without permission from the actual artist. Typologies where counterfeiting has begun to emerge in the NFT market include:

a. Minting NFTs using another artist's work (sometimes with slight changes).
b. Copying certain source code used to generate NFT Media and using it without permission.[23]
c. Creating fake websites that redirect NFT purchase payments from legitimate websites.
d. Exploiting vulnerabilities on an artist's legitimate website to post counterfeit NFTs for sale.[24]

2. Combatting Counterfeit NFTs

Many NFT marketplaces place the burden of identifying and reporting counterfeit NFTs on the artists themselves.[25] However,

15 https://cointelegraph.com/news/bored-ape-yacht-club-nfts-stolen-in-instagram-phishing-attack.
16 https://www.irs.gov/pub/irs-utl/j5-media-release-4-28-2022.pdf.
17 https://www.ssb.texas.gov/sites/default/files/2022-05/FlamingoPressRelease.pdf.
18 https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-charged-first-ever-digital-asset-insider-trading-scheme.
19 https://www.coindesk.com/business/2022/06/04/yuga-labs-confirms-discord-server-hack-200-eth-worth-of-nfts-stolen/.
20 https://www.justice.gov/usao-cdca/pr/justice-department-announces-enforcement-action-charging-six-individuals-cryptocurrency.
21 https://www.forbes.com/sites/forbestechcouncil/2021/06/29/nfts-are-fueling-authenticity-for-digital-assets-and-have-the-potential-to-create-new-use-cases/?sh=ed0fad31ffca.
22 https://www.coindesk.com/layer2/2021/12/20/nft-forgeries-arent-going-away/.
23 https://cointelegraph.com/news/fidenza-artist-slams-knock-off-nft-project-from-honest-pirates-on-solana.
24 https://www.cnet.com/news/fake-banksy-nft-sells-for-nearly-340k-after-hacker-reportedly-taps-into-artists-site/#:~:text=A%20hacker%20reportedly%20took%20advantage,minus%20a%20%245%2C000%20transaction%20fee.
25 https://www.yahoo.com/now/nft-forgeries-aren-t-going-193414909.html#:~:text=In%20a%20tweet%20thread%20last,OpenSea%2C%20all%20without%20her%20permission.&text=(NFTs%20are%20non%2Dfungible%20tokens,digital%20assets%20on%20a%20blockchain).

more can be done. NFT marketplaces should consider implementing additional mechanisms to combat counterfeit NFTs, including the following:

a. Maintaining a database of artists' work that is already posted on the platform, using image-matching technology to scan new NFTs against the database for similar images and notifying artists when their images have been minted as new NFTs.
b. Implementing due diligence procedures to verify NFT sellers' accounts and creating a system to notify buyers that the art sold through that account is verified as authentic.
c. Creating a shared register of known instances of art that has been used in counterfeit NFTs to alert other platforms to conduct heightened due diligence on the person attempting to sell NFTs using such art.
d. Scanning for embedded digital signatures, watermarks or fingerprints, or employing technology that assesses the rarity of the underlying pixel patterns of the NFT's data.[26]

Buyers can also protect themselves by:

a. Analyzing the websites that purport to be "official" NFT stores for artists or brands.
b. Researching whether certain brands or artists have sponsored campaigns or released official commentary regarding which platforms are official sellers of their artwork.
c. Monitoring whether the artist or platform has released information regarding the numbers of NFTs that have been officially minted for sale and how many have been sold to date.

Combating Insider Trading

Insider trading on NFT marketplaces is a serious risk. For example, employees may use insider information to purchase exclusive NFTs before they are available to the public and later sell them for a profit when prices spike.[27] Insiders may also provide sensitive information regarding surprise drop times or use their permissions to grant early access to friends and family. Some steps NFT marketplaces can take to prevent insider trading include the following:

1. **Formal policies.** Implement a written policy that prohibits the use of insider information, defines "insider" and "insider information," and clearly articulates prohibited conduct.
2. **Training.** Educate employees regarding what constitutes insider information and its inappropriate uses and communicate the consequences of insider trading.
3. **Monitoring.** Create an internal "watchdog" position to oversee and review NFT purchases and sales by marketplace insiders.
4. **Controls.** Implement controls such as requiring permission in instances where employees seek to buy or sell NFTs and implement technology to automatically flag transactions by insiders for review.
5. **Reporting.** Require employees to periodically submit a list of their cryptocurrency accounts and the NFTs they own with attestations that the NFTs were bought with access to publicly available information only. NFT marketplaces should consider restricting employee trading only to identified accounts and take corrective and disciplinary action against employees who trade using unreported accounts.
6. **Blackout periods.** Restrict employee transactions in certain NFTs sold on the NFT marketplace at specific times, such as the weeks around particular NFT drops.
7. **Hotlines.** Provide anonymous reporting lines for employees to share information and quickly investigate insider trading tips.[28]
8. **Firewalls.** Separate duties or create informational walls between employees responsible for preparing NFTs for launch and departments related to sales.

Market Manipulation

1. Spoofing and Shill Bidding

Spoofing occurs when a fraudster creates a high volume of fictitious buy or sell orders that tricks average traders into thinking large or high-volume transactions are occurring. Average traders panic and rush to do what they believe the market is doing and are often coerced into selling cheap or buying high to create more favorable conditions for the fraudster. Once the market moves, the fraudster cancels the fictitious order(s). Spoofing is often executed using algorithms and bots.

In the NFT context, spoofing can occur when a fraudster uses "dummy" accounts to place large volumes of low bids on NFTs to coerce the seller to sell at a lower price. Once a bid is accepted, the fraudster cancels the order and the seller must relist it, but the

26 https://www.incoproip.com/nft-fakes-scams-brand-protection/.
27 https://www.artnews.com/art-news/news/insider-trading-nft-marketplaces-regulation-1234604209/.
28 https://www.diligent.com/insights/insider-trading/five-best-practices-to-prevent-insider-trading/; https://s2.q4cdn.com/686132520/files/doc_downloads/policies/Insider-Trading-Compliance-Policy-(Shake-Shack-Inc)-Final-Approved-1-15-15.pdf.

low bid creates a new price floor and the fraudster then uses their "real" account to purchase at the lower price.

A similar technique is shill bidding. This is where the fraudster uses another account or has family and friends bid on their NFT to artificially drive up the price.[29] Spoofing and shill bidding rig the market to the detriment of honest buyers and sellers.

2. Wash Trading

Wash trading occurs when a fraudster opens multiple accounts and conducts a series of trades with themself to create artificial pricing and trading volume. The NFT is then sold to traders who think the artificial prices and buyer interest will continue. Another wash trading scenario occurs when an NFT seller mints an NFT and sells it to themself for a specific price to create artificial market demand. The seller then sells the NFT to another buyer for a significantly lower price, making it seem as though the buyer is getting a good deal, but the entire value was artificially created.[30]

3. Pump and Dump

NFTs are also susceptible to classic pump-and-dump schemes. In the NFT context, traders use social media to rally attention around the NFTs and "pump up" demand and the price. The traders then "dump" the overvalued assets for a profit and the NFTs' prices fall once the NFTs are in the hands of honest buyers.

4. Combating Market Manipulation

NFT marketplaces should consider implementing automated monitoring tools to identify potential market manipulation risks. These tools can perform functions such as:

a. Detect bot bid activity, such as when a larger number of bids than manually possible are being placed or when a pattern of large orders and audit cancellations occur related to specific accounts or NFTs.
b. Flagging transactions where the chain of custody ends with the same person who initiated the sale.
c. Identifying suspicious activity among accounts of related individuals.
d. Notifying marketplace users watching an NFT when the NFT ends up with the same seller.[31]

NFT buyers can also take steps to protect themselves, including the following:

a. Learn how to identify spoofing and shill bidding patterns, including bidding and cancellation activity.
b. Watch for bidders who immediately outbid them every time and review orders placed in the previous few days to identify whether reorders suddenly change or disappear on a regular basis.
c. Trace NFTs that were traded at a rapid pace and suddenly stopped to identify any connection between the original seller and end-user NFT wallets/accounts.
d. Identify users who buy and resell NFTs amongst themselves.[32]
e. Limit participation to NFT marketplaces that use automated systems to prevent market manipulation and take other steps to prevent fraudulent activity.
f. Recognize that order books that appear too good to be true likely are.[33]

FCPA and Bribery Concerns

The Foreign Corrupt Practices Act (FCPA) makes it a crime to make a payment, offer or promise to pay, or authorize a payment of money or anything of value directly or indirectly to any foreign official, politician, party official or candidate for office with a corrupt intent for the purpose of influencing one of these persons' official acts or decisions in violation of their lawful duty to obtain or retain business. While under-the-table cash payments represent the classic example of bribery, the FCPA prohibits the payment of anything of value, which would include gifts of NFTs, sensitive information regarding upcoming sales of NFTs or the payment of cryptocurrency to fund purchases of NFTs.

Any business that operates abroad is at risk for FCPA violations. However, businesses that are particularly at high risk are those engaged in contract procurement in the natural resource, infrastructure and defense, and pharmaceutical fields. These businesses often operate in geographic locations where it is customary or competitively advantageous to pay bribes and there is little to no anti-bribery regulation or enforcement.[34] Companies

29 https://news.bitcoin.com/are-nft-sales-susceptible-to-shill-bidding-nft-skeptics-think-its-possible/.
30 https://tittlepress.com/crypto/834147/.
31 https://moguldom.com/384308/new-study-nft-prices-are-manipulated-by-few-with-wash-trades-artificial-demand/.
32 https://cyberscrilla.com/top-tips-to-avoid-being-scammed-when-dealing-with-nfts/#:~:text=The%20classic%20pump%20and%20dump,price%20of%20an%20asset%20up; https://www.uts.edu.au/news/business-law/beware-wolf-cryptocurrency-markets.
33 https://medium.com/formosa-financial/what-is-spoofing-what-every-crypto-trader-must-know-to-protect-their-money-93706818340a.
34 https://www.ganintegrity.com/blog/compliance-risk-assessment-industry-risks/; https://www.traceinternational.org/trace-matrix.

with FCPA compliance programs should update those programs to address cryptocurrency- and NFT-related FCPA risks. The following are some examples:

1. **Disclosures.** Update due diligence and risk assessments on third-party entities and their principals, require disclosure of active cryptocurrency and NFT activity, and state its purpose and industry connection.[35]
2. **Explicit references.** Explicitly reference cryptocurrency and NFTs as a form of prohibited payments or gifts to foreign officials that can subject employees to corrective or disciplinary action.
3. **Training.** Provide periodic anticorruption compliance training and education to employees regarding the specific types of cryptocurrency and NFT transactions that violate the FCPA and require annual certification of compliance with the FCPA.[36]
4. **Reporting.** Implement a periodic employee questionnaire inquiring whether employees own cryptocurrency or NFTs, whether they use company devices to access cryptocurrency accounts or NFT platforms, and whether they have conducted cryptocurrency or NFT transactions in high-risk jurisdictions.[37]
5. **Permissions.** Define the employees within the company who can conduct business in cryptocurrencies and NFTs, which wallet addresses are allowed for corporate use, and who may receive payments.
6. **Monitoring.** Implement procedures to monitor traditional company bank accounts for transfers that involve the purchase of cryptocurrencies or NFTs.
7. **Hotlines.** Establish anonymous reporting mechanisms to collect information regarding possible or solicited bribes, educate employees on how to report bribes that take the form of cryptocurrencies or NFTs, and quickly investigate potential violations.[38]

35 https://www.foley.com/en/insights/publications/2015/12/best-practices-to-avoid-common-fcpa-violations-thi.

36 https://www.corporatecomplianceinsights.com/cryptocurrencies-instruments-for-payments-or-corruption/.

37 https://www.natlawreview.com/article/record-level-fcpa-enforcement-2020-highlights-key-risk-areas; https://www.lexisnexis.com/en-us/professional/risk-management/resources/fcpa-compliance-with-due-diligence.page.

38 https://1.next.westlaw.com/5-502-4418?transitionType=Default&contextData=(sc.Default)&__lrTS=20171105085831804&firstPage=true&OWSessionId=986b88b285e2449c8bd02871dc469bcf&fromAnonymous=true&bhcp=1.

Digital Trade-Based Money Laundering

Auction houses that have traditionally operated in the physical art space and have since incorporated NFTs into their inventory are subject to the reporting requirements of the Bank Secrecy Act (BSA) as a "financial institution," as amended by the Anti-Money Laundering Act of 2020. In some circumstances, NFT market actors may be subject to the BSA; however, regardless of whether the BSA applies to a particular activity, there is a real risk that the NFT market will enable a new form of "digital trade-based money laundering," where NFTs are used to store, move and obfuscate the source of funds derived from illegal activity. Even in the absence of a legal/compliance risk, there are business and reputational risks that NFT market actors should consider. For this reason, regardless of their BSA obligations, NFT marketplaces and related businesses should consider implementing programs to detect and prevent the use of NFTs in money laundering. Measures to consider include the following:

1. **Information collection and sharing.** Create registries of stolen or fraudulently purchased NFTs and high-risk persons or NFT wallets/public keys and make such registries accessible to other NFT ecosystem participants.
2. **Customer due diligence.** Implement policies to collect customer information, including official government identification documents, to conduct customer due diligence, combat anonymity and identify high-risk customers.
3. **Transaction monitoring.** Apply automated systems and data analytics to detect potentially suspicious activity, such as high-frequency transactions in large sums from many accounts to buy a single NFT, consecutive high-value buying and selling of NFTs in a short period of time, wallets that do not match customer profiles, wallets involved in transactions over a certain threshold, and periodic testing to assess whether new controls are needed.
4. **Written policies.** Implement a written anti-money laundering policy, including procedures for internal reporting, documenting and investigating potential money laundering, and training for employees to recognize potentially suspicious activity.

NFT Fraud Typologies

Fraud schemes involving NFTs operate like any other fraud scheme – a person is deceived into departing from something of value and receives little to nothing in return, to the enrichment of the fraudster.

NFT fraud schemes may be advertised on social media platforms to rally attention, marketed with legitimate-looking websites and even employ online chat function technology to lure victims. Examples of fraud typologies that may arise in the NFT market include the following:

1. **Fraudulent NFT sales.** A fraudulent NFT seller never delivers the NFT to the buyer or delivers something not promised.[39]
2. **Fraudulent inducement.** A fraudster contacts a vulnerable victim, such as an elderly individual or someone with no cryptocurrency experience, and uses a scheme to convince the victim into completing an NFT or a cryptocurrency transaction that inures to the benefit of the fraudster.[40] Examples of schemes fraudsters may use include impersonating a friend or family member, purporting to represent a legitimate enterprise (including an NFT trading platform), a romance scam or a fake contest prize.
3. **Investment schemes.** A fraudster claims they manage an investment vehicle to pool assets and invest in NFTs. The victim invests in the form of cryptocurrencies and the fraudster absconds with the funds. Alternatively, when the victim tries to make a withdrawal, the victim is asked to pay "withdrawal fees" to withdraw their assets.
4. **Ponzi schemes.** A fraudster claims to manage NFT investments and perpetuates an investment scheme that promises high and quick returns. When a victim requests to cash out the value of their NFT "profits," they are paid with the cryptocurrency of other investors.

NFT market participants can defend against fraud by conducting due diligence on NFT sellers and other third parties and by watching out for common signs of fraud, including (1) typographical errors and obvious misspellings in emails, social media posts or other communications; (2) promises to multiply the investment; (3) promises of free money; (4) secretive or complex strategies and fee structures; (5) fake influencer- or celebrity-led social media campaigns; (6) reluctance to grant access to account information; and (7) errors in account statements.[41]

Conclusion

As the NFT market continues to expand, new NFT fraud risks and fraud typologies are likely to develop as well. By understanding the risks and taking informed, measured steps to combat fraud and corruption, NFT market participants can promote NFT technology and reap the rewards of the associated opportunities while steering clear of events that would disrupt and damage their business. More importantly, by implementing programs to combat fraud and corruption, NFT market actors can promote healthy market growth and help innocent consumers avoid losses.

39 https://www.cointribune.com/en/analysis/cybersecurity/17-year-old-artist-sells-144000-worth-of-fake-nfts/.

40 https://www.vancouverislandfreedaily.com/news/fraudsters-spoof-oceanside-rcmp-number-to-lure-resident-into-cryptocurrency-scam/.

41 https://www.sec.gov/files/ia_virtualcurrencies.pdf.