Finanšu izlūkošanas dienests

Vaļnu iela 28, Riga, LV-1050; tel. +371 67044430; e-mail: fid@fid.gov.lv; www.fid.gov.lv

MONEY LAUNDERING, TERRORISM AND PROLIFERATION FINANCING RISKS OF NFTS

STRATEGIC ANALYSIS STUDY

2022

Table of contents

Introduction

The Financial Intelligence Unit of Latvia has carried out a preliminary study on the money laundering (ML), terrorism and proliferation financing (TF/PF) risks associated with a type of virtual asset - non-fungible tokens (NFTs).

NFTs are unique blockchain-based digital certificates that represent ownership of various types of physical or digital property. By accessibly enabling verifiable ownership records and enabling creators to earn royalties after the original sale of the digital asset – the NFT market is becoming one of the most rapid growing sectors of the global digital economy.[1]

NFTs can be vulnerable to ML and TF/PF. As virtual asset exchanges become increasingly subject to anti-money laundering (AML) compliance, many of the associated risks are being transferred to NFT marketplaces – a quickly growing market sector with little applicable know-your-client (KYC) or transaction monitoring obligations. The absence of AML obligations in NFT marketplaces produce risks to the users of the platforms, and financial integrity more broadly.

Many of these risks are tied to a lack of clarity in the regulation of NFTs. As each NFT is unique to its underlying asset or function, NFTs can be utilized in numerous market segments, ranging from fine art to financial services. This regulatory opaqueness is creating gaps in ML/TF/PF monitoring and enforcement.

This study outlines several emerging vulnerabilities in the NFT domain. Self-laundering, wash trading, and tax fraud are a few examples of resultant emerging typologies. The study includes case examples and ML typologies with the usage of NFTs.

As NFTs increase in popularity and use cases, FIU Latvia recommends cryptocurrency exchanges to pay increased attention to suspected NFT wallets and transactions. Exchanges may also aim to encourage the use of transparent cryptocurrencies for the trade of NFTs. However, as NFT market evolves a secondary market, more concrete regulatory stances may be necessary to prevent the increase of ML and TF/PF risks in the virtual asset market.

[1] The NFT market surpassed USD 40 billion in 2021 according to some estimates. See "NFT Market Surpassed $40 Billion in 2021, New Estimate Shows". Available: https://www.bloomberg.com/news/articles/2022-01-06/nft-market-surpassed-40-billion-in-2021-new-estimate-shows

1. Market Overview

1.1. The NFT market is growing rapidly. Close to $41 billion worth of cryptocurrency in NFT transactions has been tracked in just one blockchain protocol, with exponential year-to-year growth from 2019.[2] Though NFTs are based on the same blockchain technology as cryptocurrency,[3] they differ by being non-fungible. NFTs are unique certificates minted on the blockchain associated with a certain digital object.[4] Most commonly, this digital association represents underlying ownership of a digital or physical asset, including images, videos, audio files, or other property. The functions of NFTs are managed with smart contracts and digital wallets, and generally, these actions are publicly verifiable and auditable, as they are recorded on the underlying blockchain.

1.2. NFT creation is very accessible. Known as "minting" – NFTs are created via submitting code directly into specific underlying blockchain with data on the proprietary asset, terms, and wallet address.[5] Generally any individual with a wallet address can mint, hold, transfer, and - depending on the underlying blockchain - delete (known as "burning") the NFT. Blockchains differ by functionality, from requiring additional metadata to creating restricted NFT subnets. Through blockchain interoperability services (known as "bridges"), NFTs can be moved across blockchains by "locking" them on the initial blockchain and recreating them in the new one.[6]

1.3. NFTs can be traded in a variety of avenues. They can be sent from wallet to wallet directly, without third-party involvement, but can also be guided by physical intermediaries. A recent sale of a high-profile NFT involved, for example, Beeple's Everydays: The First 5000 Days, which sold at Christie's auction for more than $69 million.[7] Most of the NFT trade, however, takes place in marketplaces such as OpenSea, LooksRare, and SuperRare, which function similar to auction houses or art dealers by connecting buyers and sellers who transact directly, using digital currency.[8] The top three digital NFT marketplaces alone have had an estimated lifetime trading volume of $55 billion.[9]

1.4. The NFT trade is also evolving a secondary market. Through the use of smart contracts, NFTs are being split into fractionalized NFTs (F-NFT) that represent ownership of the whole. F-NFTs function similarly to fungible crypto-assets, with similar utility including staking or voting rights. F-NFTs do not destroy the initial NFT, but instead lock them into a smart contract that can only be unlocked with the ownership of the fractions.

---

[2] NFT Money Laundering and Wash Trading. Available: https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-nft-wash-trading-money-laundering/

[3] Blockchain is a digital, additive ledger that is duplicated and distributed across all network participants, ensuring a means of decentralized storage and preventing modifications of previous entries. Data in blockchain is stored in sequential batches called 'blocks' that – when filled to capacity with data – create new blocks that are connected to the previous block. See "The Truth About Blockchain". Available: https://hbr.org/2017/01/the-truth-about-blockchain

[4] NFTs generally have three core characteristics; 1) they represent a unique object which can be unequivocally associated with a virtual wallet, 2) they are not replicable or interchangeable, and 3) they cannot be divided into parts. See "What You Need to Know About Non-Fungible Tokens (NFTs)". Available: https://www.forbes.com/uk/advisor/investing/cryptocurrency/nft-non-fungible-token/

[5] Ethereum, Avalanche, and Binance Smart Chain are just a few of the popular blockchains supporting the minting of NFTs.

[6] From Ethereum to Solana and Back: Wormhole Lets You Send Your NFTs Across Blockchains. Available: https://decrypt.co/81764/ethereum-solana-wormhole-send-nfts-across-blockchains

[7] Beeple Sold an NFT for $69 Million. Available: https://www.theverge.com/2021/3/11/22325054/beeple-christies-nft-sale-cost-everydays-69-million

[8] See opensea.io, looksrare.com, or superrare.com.

[9] NFT (Non-Fungible Tokens) Marketplaces. Available: https://dappradar.com

Estimates of the nascent F-NFT market place its total market cap at around $100 million.[10]

1.5. Though NFTs are most associated with art-collectibles, their utility is quickly expanding. They are being used as the base for digital rights management,[11] authenticity verification,[12] or supply chain management.[13] Through these utilities, NFTs are rapidly integrating into different sectors, like precious goods, gambling, or gaming.

[10] Fractionalized NFTs Market Cap. Available: https://dappradar.com

[11] DeFi Lending Hub Goldfinch Fuses NFTs and User IDs to Attract Wary Investors. Available: https://thedefiant.io/nfts-kyc-goldfinch-identity/

[12] Diamond companies, for example, are using blockchain to trace their diamonds. See "De Beers Group Introduces World's First Blockchain-Backed Diamond Source Platform at Scale". Available: https://www.debeersgroup.com/media/company-news/2022/de-beers-group-introduces-worlds-first-blockchain-backed-diamond-source-platform-at-scale

[13] New Platform Uses NFTs as a Gateway for Digital Rights Management. Available: https://www.zdnet.com/finance/blockchain/new-platform-uses-nfts-as-a-gateway-for-digital-rights-management/

2. Regulatory Framework

2.1. As NFTs are mostly transacted using cryptocurrency, they are indirectly affected by rules on virtual assets and VASPs. For example, to purchase the most commonly used crypto currency for the trading of NFTs – Ethereum – individuals entering the market are likely to exchange fiat currency into cryptocurrency at a regulated Virtual Asset Service Provider (VASP). Exchanging proceeds from NFT trade back into fiat currency will usually also take place at a VASP.

2.2. At the moment, NFTs remain generally unregulated. The FATF positions that the most common NFTs used as collectibles are a "crypto-collectible" and are generally not considered virtual assets.[14] Their creators also do not qualify as VASPs.

2.3. However, the FATF notes that NFTs may fall under the definition of virtual assets if used for payment or investment purposes in practice. NFTs that are, for example, digital representations of other financial assets already covered in the FATF Standards should be covered by rules for that financial asset. The application of FATF standards to NFTs should thus be considered on a case-by-case basis,[15] an approach reflected in several jurisdictions.

Latvia

2.4. Under the Latvian AML regime, NFTs remain unregulated. Digital assets are defined under the concept of "virtual currency" – a "digital representation of value" that can "operate as a means of exchange."[16] The general interpretation is that as long as NFTs are not inherently used for payment functions, they are outside the scope of virtual currencies.

France

2.5. French regulation creates a broader framework for classifying digital assets.[17,18] Under French law, NFTs are likely to be classified as a utility token - a digital asset representing "one or more rights, which can be issued, recorded, stored or transferred by means of a shared electronic recording device allowing the owner of the asset in question to be identified, directly or indirectly."[19]

2.6. However, NFT marketplaces do not qualify as VASPs under French law, unless they provide a secondary market for digital storage services, allow purchase or sale of digital assets in legal tender, offer service of exchange of digital assets for other digital assets, and operate a platform for trading of digital assets.[20]

---

[14] Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (2021). Available: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

[15] Id.

[16] Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing, Section 1, Paragraph 1, Clause 2^2. Available: https://likumi.lv/doc.php?id=178987

[17] Digital assets are defined by the Code Monétaire et Financier. The other form of digital assets is payment token - any digital representation of value that is not issued or guaranteed by a central bank or public authority, is not necessarily linked to a legal tender, and does not have the legal status of money but is accepted by natural and legal persons as a medium of exchange that can be transferred, stored, or exchanged electronically. See "LOI N° 2019-486 Du 22 Mai 2019 Relative à La Croissance et La Transformation Des Entreprises". Available: https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000037080861/

[18] Supra note 14.

[19] Id.

[20] Id.

United States

2.7. A recent study by the U.S. Department of the Treasury notes that NFT platforms like Dapper Labs, SuperRare, and OpenSea may qualify as VASPs depending on the "nature and characteristics" of offered NFTs. Though NFTs used in practice as collectibles may not fall under the definition of virtual asset, NFT marketplaces may qualify as VASPs if the NFTs are used for payment or investment purposes. This is linked, in particular, to FinCEN's regulation not limiting the scope of the term "value that substitutes for currency."[21]

2.8. Similarly, platforms doing business transferring virtual assets during the buying or selling of NFTs may have U.S. AML/CFT obligations under FinCEN's rules for money service businesses if they are doing business in the United States.[22] Fractional-NFT interests could be securities and be subject to securities regulation, as it changes NFTs into a fungible asset, and possibly an investment security.

United Kingdom

2.9. In the United Kingdom, an NFT is categorized by the Financial Conduct Authority (FCA) as an "unregulated token."[23] Such tokens, including utility tokens, are used to purchase services, access a distributed ledger technology platform, or exchange tokens. However, if they exhibit characteristics akin to other forms of crypto asset, their categorization will change accordingly.

2.10. Under the UK AML framework, crypto asset exchange providers and custodian wallet providers are required to register with the FCA before undertaking crypto asset activities, broadly defined to capture any

"…cryptographically secured digital representation of value or contractual rights that uses a form of distributed ledger technology and can be transferred, stored or traded electronically."[24]

2.11. Platforms that provide NFT exchange services may also be required to register under the FCA, thus coming under AML rules.

2.12. In practice, NFTs are at a crossroads between fine art and cryptocurrency sectors, both of which are coming under increasing regulation. However, at the moment, neither art, nor cryptocurrency rules are directly applicable to NFTs. As NFTs enter and bring utility to new markets, similar regulatory gaps may follow.

2.13. Following this logic, certain regulators have compared NFT marketplaces to fine art dealers. However, they differ in structure, ownership models, operations, standards and due diligence protocols. An agency problem also disincentivizes platforms from verifying buyer identities, as the platform may generate revenue from transactions made by clients using the platform.

2.14. However, much supervisory capacity is at the point of exchange between Fiat currencies and cryptocurrencies. Known as "on- and off-ramps" – these currently remain the main points of supervisory attention, as VASPs are increasingly regulated

---

[21] It can be created for specifically the purpose of being used as a currency substitute or originally for another purpose but then repurposed to be used as a currency substitute by centralized or decentralized payment systems. See "Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art (2022)". Available: https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf

[22] FinCEN's regulation does not limit or qualify the scope of the term "value that substitutes for currency." It can be created either (a) specifically for the purpose of being used as a currency substitute, or (b) originally for another purpose but then repurposed to be used as a currency substitute by centralized or decentralized payment administrator. For a discussion, see Id.

[23] The Financial Conduct Authority specified three types of cryptoassets, the other two are E-money tokens and security tokens. See "Guidance on Cryptoassets (2019)". Available: https://www.fca.org.uk/publication/policy/ps19-22.pdf

[24] HMRC internal manual: Cryptoassets Manual. Available: https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10100

and are putting in place KYC and CDD measures.[25] They are especially important for the detection of large incoming and outcoming sums of money, typical in NFT transactions.

[25] Virtual Currencies: Money Laundering and Terrorism and Proliferation Financing Risk Assessment (2021). Available: https://www.fid.gov.lv/uploads/files/2021/virtu%C4%81l%C4%81s%20val%C5%ABtas/VIRTUAL%20CURRENCIES.pdf

3. Risks

3.1. NFTs present a range of ML/TF/PF risks. These include traditional fraudulent activities, such as forging NFTs and misleading buyers.[26] These risks are especially pertinent in NFT marketplaces, which operate using automated smart-contracts, with minimal KYC requirements, and rarely institute any monitoring mechanisms.[27] However, NFTs also exhibit many risks from their similarities to the art market. These include anonymity, off-record sales, and the involvement of high-risk jurisdictions. Many of these risks are bolstered in the unregulated trade of NFTs without intermediaries, where they can support ML/TF asset fundraising, stockpiling, or sanctions evasion.

Vulnerabilities

3.2. NFTs present several vulnerabilities interlinked with their art characteristics and the underlying blockchain technology.

3.3. The first vulnerability is the art trade characteristics of the broader NFT domain. In the lightly regulated NFT market, these characteristics include a high level of buyer secrecy and information, self-regulated markets, non-transparent pricing, and high value transactions. These aggregate into a high propensity for large-value transactions between unknown parties, as well as leaving gaps for a variety of fraudulent activity in NFT marketplaces and other avenues.

3.4. The second vulnerability is the ease of NFT ownership transferability integral to the underlying blockchain technology. Like cryptocurrencies, transferring ownership of NFTs is not delimited by geographical boundaries, and takes place without the potential of regulatory intervention or cost. NFT ownership can thus rapidly change between different wallets and ultimate beneficiaries. This makes registering assets by tax or other authorities very difficult, as the jurisdictional status of an NFT is unclear.

3.5. The third vulnerability is in the concealability of underlying cryptocurrency transactions. While the change of NFT ownership between digital wallets can be traced, a change in wallet address does not reflect change in ownership. As most major NFT platforms do not require KYC or perform customer due diligence, true beneficial wallets have to be mapped via their transaction blocks, to see the chain of digital wallets through which currency has passed. This process is made more complex by cryptocurrency "mixers" or "tumblers" that circulate a wallet's cryptocurrency through numerous transactions across different blockchains thus "washing" it from potential connection to suspicious wallets and transactions.[28] NFT transactions themselves could also be used for tumbling, especially if circulated through the variety of secondary markets or derivatives, like F-NFTs.

3.6. The fourth vulnerability is the ease of hiding wallet ownership. Once the ultimate beneficiary wallets are located, they need to be assigned to a legal or natural person. Cryptocurrency wallets, however, are inherently pseudonymous, and identifying the responsible individual may require identifying the relevant IP address, employed hardware, and other factors that may involve various jurisdictions.

[26] A hacker allegedly exploited the website of the artist 'Banksy' to sell a forged NFT through his website. See "Fake Banksy NFT Sold through Artist's Website for £244k". Available: https://www.bbc.com/news/technology-58399338

[27] For example, they are outside of the scope of the European Union MiFID and MiFIR or the US Anti-Money Laundering Act of 2020 that expands its definition of financial institutions to include business involved in the exchange of "value that substitutes for currency or funds".

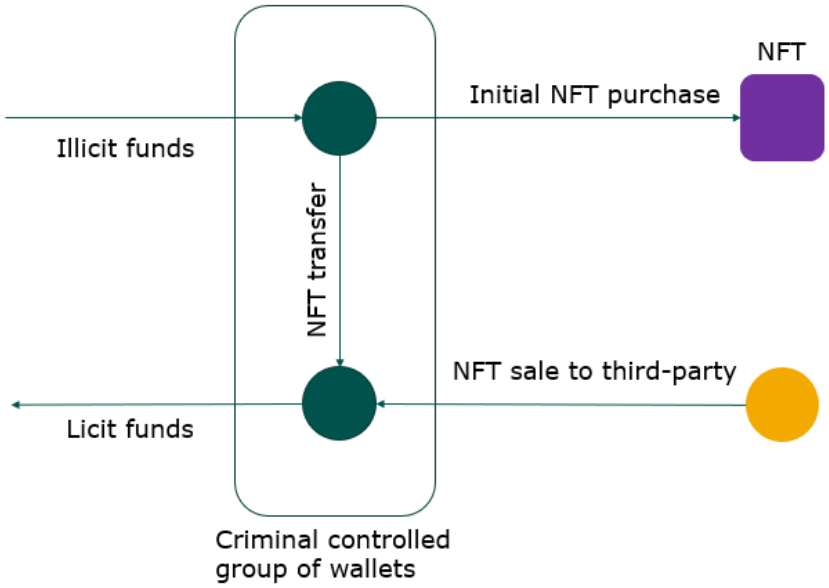
[28] Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (2019). Available: https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models

4. Typologies

4.1. Several typologies are emerging in NFT trade and marketplaces tied to ML/TF-based and a variety of other predicate crimes. These typologies reflect patterns encountered in the art and cryptocurrency segments, but also reflect the utilization of NFTs in different markets, like decentralized finance or gambling.

4.2. **Self-laundering.** A criminal can purchase an NFT with illicit funds, and then transfer it to another digital account to create a record of sales on the blockchain. By selling it to an unsuspecting buyer, the criminal can withdraw funds and layer them into the licit economy on the other end.[29] Criminals can also purchase their own NFTs without a third-party, and use such trading to establish a licit source of funds.

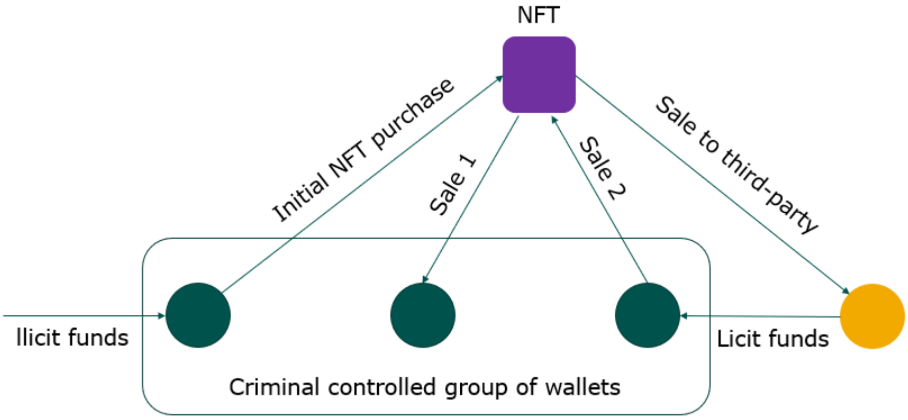
Figure 1
Self-Laundering



4.3. **Wash trading.** Criminals can engage in trades over a certain NFT taking place between multiple wallets controlled by them to slowly inflate its value over multiple transactions and give an illusory view of trading volume and open interest in the NFT. The final sale of the NFT to a victim for a much higher price become fraudulent proceeds for the wash traders. The wash trading can take place with an NFT under the initial control of the criminals, or an unsuspecting NFT owner.[30]

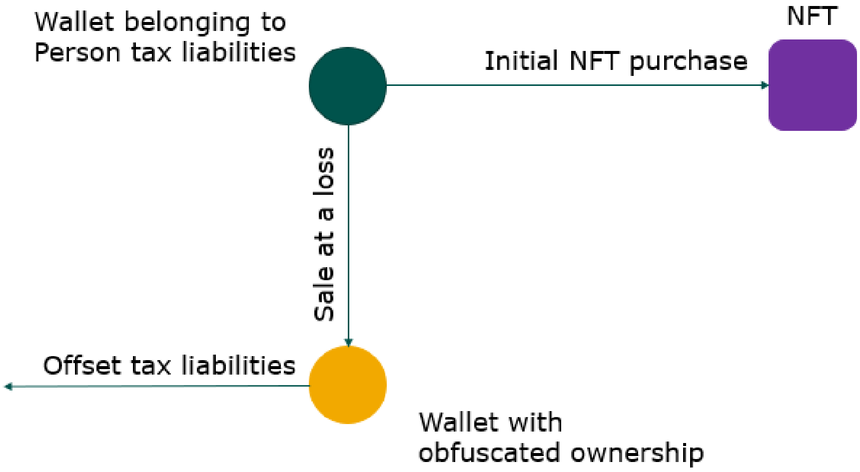
[29] Supra note 21.
[30] NFT Wash Trading: Quantifying Suspicious Behaviour in NFT Markets (2022). Available: https://www.researchgate.net/publication/358458335_NFT_Wash_Trading_Quantifying_suspicious_behaviour_in_NFT_markets

Figure 2
Wash Trading



4.4. **Tax fraud.** An account with a large tax liability buys an NFT from an unknown account. The account then sells to a third account for a significantly lower price, realizing a loss that offsets the previous tax liabilities. The identity of the participants' accounts is obfuscated via anonymous cryptocurrency and tumblers.[31]

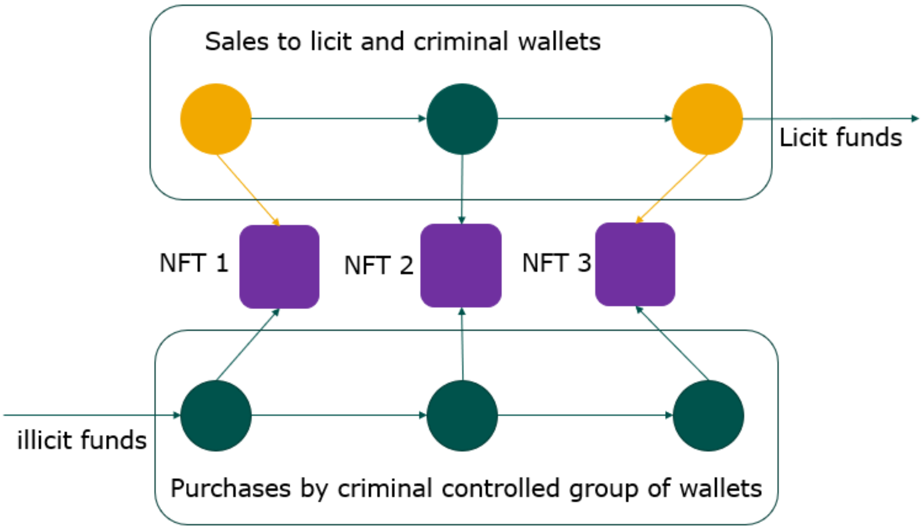
Figure 3
Tax Fraud



4.5. **Smurfing.** Criminals purchase a large amount of cheaper and unrelated NFTs created and controlled by them with illicit funds to create a record of sales over a longer period of time. These wallets can then sell the NFTs to each other and slowly extract smaller amounts of money through cryptocurrency exchanges into fiat.[32]

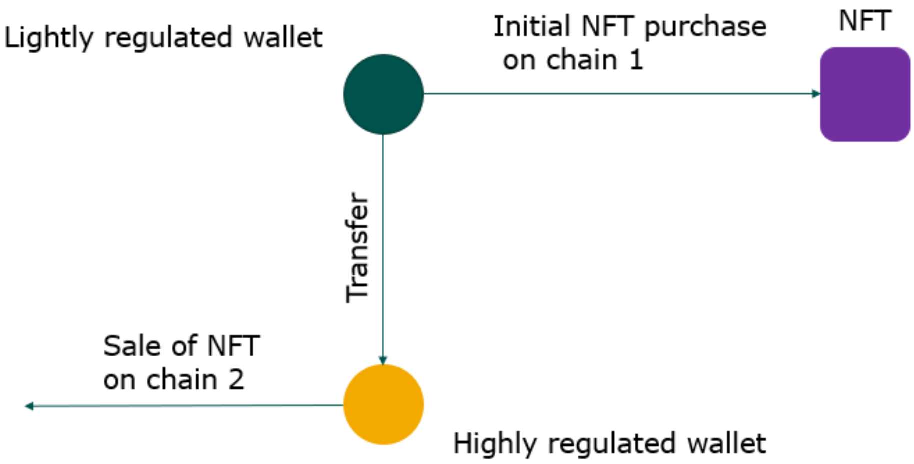
[31] IRS Views NFTs as Tax Evasion Threat, but Cryptocurrency Experts Disagree. Available: http://www.proquest.com/docview/2534502639?pq-origsite=gscholar&fromopenview=true
[32] For a discussion of smurfing via crypto assets and NFTs, see Europol. See "Two Criminal Groups Dismantled for Laundering EUR 2.5 Million through Smurfing and Cryptocurrencies". Available: https://www.europol.europa.eu/media-press/newsroom/news/two-criminal-groups-dismantled-for-laundering-eur-25-million-through-smurfing-and-cryptocurrencies

Figure 4
Smurfing



4.6. **Sanctions evasion.** A sanctioned wallet 'locks' and transfers an NFT to a different unsanctioned digital wallet by recreating the NFT in a new blockchain with a different wallet used on exchanges that have lighter or no KYC requirements. This new wallet can then trade with the NFT.[33]

Figure 5
Sanctions Evasion



[33] For a discussion of sanctions avoidance by cryptocurrency and NFTs. See "Measures Needed to Address NFT-Enabled Sanctions Evasion". Available: https://sanctionsassociation.org/measures-needed-to-address-nft-enabled-sanctions-evasion/

5.Case Study

NFT Case 1

5.1. A self-taught digital artist transferred several million EUR from their cryptocurrency account to their personal bank account, claiming that the source of funds is the income from selling digital art in the form of NFT. The artist's criminal past and links to organized crime raised suspicions, as did an the absurdly steep rise (and a similarly rapid decline afterwards) in the commercial success of the artist, in the period of one month rising from a digital art enthusiast to one of the most successful NFT artists. Multiple red flags appeared upon analyzing the NFT transactions. The red flags indicated possible fictitious bidding, fictitious buyers, inflated value of the artworks, as well as the use of different cryptocurrency services that reduce the traceability of transactions.

NFT Case 2

5.2. In 2021, a wallet holder sold a single NFT from a popular collection for several hundred thousand EUR worth of cryptocurrency. Upon investigation, it was found that soon after the sale, the buyer wallet sent the NFT back to the original owner wallet address. The same wallet then subsequently placed the NFT for sale again for an even higher price. The movement of the NFT between wallets after sale, and the increase of the sale price was indicative of fictitious buyers, and purposely inflated value of the NFT for the purpose of wash trading.

6. Risk Indicators in the Art-Collectibles NFTs

6.1. A variety of risk indicators can be indicative of ML activity using NFTs. These indicators can be mixed to use a variety of methods together.

Self-laundering[34]

6.2. Inactive or "cold" wallets becoming active for transactions with a limited range of NFTs or an NFT collection;

6.3. NFTs are sold between a limited group of wallets;

6.4. Cryptocurrency from sold NFTs does not re-enter the NFT or cryptocurrency market, but remains dormant or is converted into fiat;

6.5. A mixer is used in any part of the transaction chain.

Wash Trading[35]

6.6. Rapidly changing values for NFT trades, incoherently with other values in the series or with large non-incremental jumps in price;

6.7. A limited amount of impacted NFTs from a series or collection;

6.8. Large decreases in price of NFTs over a short period of time in the NFT marketplace;

6.9. A high number of transactions between the same or connected groups of self-financed wallets.

Tax Fraud[36]

6.10. An NFTs value incoherently decreases in value at time of sale;

6.11. Multiple NFTs belonging to a wallet or a group of wallets are sold at a loss over a period of time;

6.12. Sales of NFTs may take place within the same group of wallets.

Smurfing[37]

6.13. A variety of wallets split contained cryptocurrency (through a mixer or manually) among more wallets for no discernable purpose;

6.14. A wallet or group of wallets spend much of their available assets by purchasing many NFTs of varying series and values;

6.15. Purchased NFTs are either novel and low-value or with stable value;

6.16. Cryptocurrency from sold NFTs returns to a series of interconnected wallets.

Sanctions Evasion[38]

6.17. Wallets use unregulated exchanges or exchange with low levels of KYC to on- or off-ramp fiat;

---

[34] Supra note 14.
[35] Supra note 2.
[36] Supra note 14.
[37] Id.
[38] Supra note 2.

6.18. Wallets purchasing NFTs convert cryptocurrency from cryptocurrency with high levels of anonymity;

6.19. After selling NFTs, cryptocurrency is converted at a lightly regulated exchange or to a cryptocurrency with high level of anonymity.

7. Conclusions

7.1. The NFT market is burgeoning in both volume and innovation. Close to $41 billion worth of cryptocurrency in NFT transactions has been tracked in just one blockchain protocol, with exponential year-to-year growth from 2019, when the market was just a fraction of the size.[39] NFTs are also seeing broader adoption across a variety of sectors, both as a commodity and a utility.

7.2. These new innovations, as well as secondary markets are increasingly coming under the attention of regulators. Because of the high level of anonymity, and low level of regulation, NFTs are prone to a variety of vulnerabilities. Such vulnerabilities have much in common with the art trade market or even the earlier unregulated cryptocurrency market; the owners of NFTs are often anonymous, trades are unregistered, and underlying cryptocurrency transactions can be concealed.

7.3. These vulnerabilities, together with the light and highly variable regulation of NFTs engender a variety of ML/TF typologies. Many cryptocurrency typologies also apply to NFTs, but the non-fungible attributes lend them to new types of application. Self-laundering, wash trading, and smurfing, for example, exemplify novel ML/TF threats unique to NFT marketplaces.

7.4. There is ample space for governments to provide support for the creation and enhancement of private sector information-sharing programs to encourage transparency among NFT market participants. This can be done via applying KYC requirements for NFT marketplaces or using targeted recordkeeping and reporting requirements. However, NFT risks will remain pertinent until regulatory convergence takes place.

[39] NFT Money Laundering and Wash Trading Chainalysis (2022). Available: https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-nft-wash-trading-money-laundering/

List of abbreviations and terms

AML	Anti-Money Laundering
F-NFT	Fractional NFT
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FIU Latvia	Financial Intelligence Unit of Latvia
FinCEN	Financial Crimes Enforcement Network
KYC	Know Your Client
ML	Money laundering
NFT	Non-fungible tokens
TF/PF	Terrorism and proliferation financing
USA	United States
UK	United Kingdom
VASP	Virtual Asset Service Provider