Department of the Treasury

Illicit Finance Risk Assessment of Non-Fungible Tokens

May 2024

Department of the Treasury

Illicit Finance Risk Assessment of Non-Fungible Tokens

Table of Contents

Illicit Finance Risk Assessment of Non-Fungible Tokens

Executive Summary

The risk assessment explores how vulnerabilities associated with non-fungible tokens (NFT) and NFT platforms may be exploited for illicit finance purposes, including money laundering, terrorist financing, and proliferation financing. The assessment of NFTs was prompted by Treasury's commitment in the 2022 "Digital Asset Action Plan to Address Illicit Finance Risks"[1] to monitor emerging risks in the digital assets sector as well as by global challenges in developing and implementing anti-money laundering and countering the financing of terrorism (AML/CFT) standards for NFTs.[2] As noted in the 2024 National Risk Assessments[3] and the "Illicit Finance Risk Assessment on Decentralized Finance"[4] (DeFi Risk Assessment), this risk assessment recognizes that most money laundering, terrorist financing, and proliferation financing by volume and value of transactions occurs in fiat currency or otherwise outside the digital asset ecosystem via more traditional methods.

There is no widely agreed upon definition of an NFT given the diverse range of NFT types, uses, and designs. However, broadly speaking, an NFT is a digital unit or token with a unique identifier on an underlying blockchain that represents content that may or may not be stored on the blockchain. With regards to the market structure, the NFT risk assessment recognizes that while the NFT market grew immensely in the summer of 2021, NFT sales peaked in early-to-mid 2022, when Treasury committed to publishing the risk assessment. Since then, sales decreased sharply through the end of 2022, increased again in early 2023, and have since again declined.[5]

The assessment identifies that NFTs and NFT platforms are, to date, rarely being used for proliferation financing or terrorist financing. However, the assessment finds that NFTs are highly susceptible to use in fraud and scams, many of which are traditional schemes that involve NFTs, and can be stolen from victims. Additionally, criminals use NFTs to launder proceeds from predicate crimes, often in combination with other techniques or transactions meant to obfuscate the illicit source of funds. Criminals can exploit vulnerabilities related to characteristics of NFTs, the assets or entitlements that they reference, and regulatory frameworks in the United States and abroad. In particular, cybersecurity vulnerabilities, challenges related to copyright and trademark protections, and hype and fluctuating pricing of NFTs can enable criminals to perpetrate fraud and theft related to NFTs and NFT platforms. Moreover, some NFT firms and platforms lack appropriate internal controls to mitigate risks to market integrity, money laundering and terrorist financing, and sanctions evasion.

The assessment examined several mitigation measures, including (1) industry solutions to help platforms and

1 "Action Plan to Address Illicit Financing Risks of Digital Assets," U.S. Department of the Treasury, September 2022, https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf

2 "Targeted Update On Implementation Of The FATF Standards On Virtual Assets And Virtual Asset Service Providers," FATF, June 2022, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf; "G20 Finance Ministers and Central Bank Governors Meetings Communique," University of Toronto, February 18, 2022, http://www.g20.utoronto.ca/2022/220218-finance.html; "A deep dive into crypto financial risks: stablecoins, DeFi and climate transition risk," European Central Bank, July 11, 2022, https://www.ecb.europa.eu/pub/financial-stability/macroprudential-bulletin/html/ecb.mpbu202207_1~750842714e.en.html.

3 "Treasury Publishes 2024 National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing," U.S. Department of the Treasury, February 2024, https://home.treasury.gov/news/press-releases/jy2080.

4 "Illicit Finance Risk Assessment of Decentralized Finance," U.S. Department of the Treasury, April 2023, https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

5 Andrew Hayward, "NFT Sales in 2022 Nearly Matched the 2021 Boom, Despite Market Crash," Decrypt, January 4, 2023, https://decrypt.co/118438/2022-versus-2021-nft-sales; "NFTs and Financial Crime," Elliptic, August 24, 2022, https://www.elliptic.co/resources/nfts-financial-crime, NFTGo, "2023 NFT Market Analysis: An Insider Look," CoinMarketCap, May 2023, https://coinmarketcap.com/academy/article/2023-nft-market-analysis:-an-insider-look.

consumers identify potential scams; (2) law enforcement authorities and public announcements; (3) analysis of public blockchain data; and (4) existing regulations and requirements for industry participants, finding that they partially mitigate the identified threats and vulnerabilities associated with NFTs. The assessment also outlines several recommendations for the U.S. government and for the private sector to address outstanding risk, including for regulators to consider application of regulations to NFTs, raise awareness of existing obligations, and continue enforcing existing laws and regulations. Moreover, the assessment recommends that the U.S. government should continue private sector engagement to understand developments in the NFT ecosystem and encouraging industry to address scams suggests that both the U.S. government and private sector take further steps to educate consumers about NFTs and related risks. Lastly, the assessment recommends that the U.S. government engage with foreign partners to encourage them to assess and address the illicit finance risks of NFTs.

1. Introduction

In September 2022, the Department of the Treasury (Treasury), in line with Executive Order 14067 of March 9, 2022, "Ensuring Responsible Development of Digital Assets," published an "Action Plan to Mitigate the Illicit Financing Risks of Digital Assets" (Action Plan).[6] The Action Plan, building upon Treasury's "2022 National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing" (2022 NRAs),[7] identified illicit finance risks associated with virtual assets, including the misuse of so-called non-fungible tokens (NFTs) to launder illicit proceeds. There is no widely agreed upon definition of an NFT given the diverse range of NFT types, uses, and designs. However, broadly speaking, an NFT is a digital unit or token with a unique identifier on an underlying blockchain that represents content that may or may not be stored on the blockchain. NFTs, as discussed in more detail below, may in some cases be virtual assets[8] as defined by the Financial Action Task Force (FATF), the international standard setting body for anti-money laundering and countering the financing of terrorism (AML/CFT) and proliferation of weapons of mass destruction (CPF). NFTs, including those that are considered virtual assets, fall within the term digital asset, which includes virtual assets as well as other assets.[9]

1.2 Risk Assessment Overview

This risk assessment explores how vulnerabilities associated with NFTs and NFT platforms may be exploited for illicit finance purposes, including money laundering, terrorist financing, and proliferation financing. This assessment of NFTs was prompted by Treasury's commitment in the Action Plan to monitor emerging risks in the digital assets sector as well as by global challenges in developing and implementing AML/CFT standards for

6 "Action Plan to Address Illicit Financing Risks of Digital Assets," U.S. Department of the Treasury, September 2022, https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf; "Executive Order 14067: Ensuring Responsible Development of Digital Assets," Executive Office of the President, March 2022, https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets.

7 "Treasury Publishes National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing," U.S. Department of the Treasury, March 2022, https://home.treasury.gov/news/press-releases/jy0619.

8 "Virtual assets" are a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations.

9 The term "digital assets" refers to all CBDCs, regardless of the technology used, and to other representations of value, financial assets and instruments, or claims that are used to make payments or investments, or to transmit or exchange funds or the equivalent thereof, that are issued or represented in digital form through the use of distributed ledger technology. For example, digital assets include cryptocurrencies, stablecoins, and CBDCs. Regardless of the label used, a digital asset may be, among other things, a security, a commodity, a derivative, or other financial product. Digital assets may be exchanged across digital asset trading platforms, including centralized and decentralized finance platforms, or through peer-to-peer technologies.

NFTs.[10] Still, as noted in the 2024 NRAs[11] and the "Illicit Finance Risk Assessment on Decentralized Finance"[12] (DeFi Risk Assessment), this risk assessment recognizes that most money laundering, terrorist financing, and proliferation financing by volume and value of transactions occurs in fiat currency or otherwise outside the digital asset ecosystem via more traditional methods.

The risk assessment begins with an overview of NFTs, including their types and functions, and the NFT market. The risk assessment then describes the ways in which illicit actors are misusing NFTs before discussing the vulnerabilities they exploit to do so. Finally, the risk assessment discusses several aspects of the NFT space that may partially mitigate abuse of NFTs for illicit finance purposes. The risk assessment concludes with several recommended actions for Treasury, the broader U.S. government, and the private sector.

This assessment does not alter any existing legal obligations, issue any new regulatory interpretations, establish any new supervisory expectations, nor create or confer any legal rights, privileges, or benefits that may be enforced in any way by private parties. The terms used in this report are intended to reflect the meanings commonly used by the industry and market participants with modifications and clarifications as appropriate. All definitions discussed in this assessment apply only within the scope of this assessment. They are intended only to facilitate an understanding of NFTs and associated risks. Nothing in this assessment affects the obligations of any of the participants described herein under other regulatory frameworks, for example, the federal securities laws.

2. Market Structure

2.1 Definition & Scope

NFTs are technologically unique, verifiable digital units or tokens that are recorded on a blockchain and are often purportedly used to certify authenticity or represent ownership of certain rights or assets. NFTs claim to represent ownership of various forms of media, real estate, access rights, and intellectual property, among other uses; however, an NFT may in reality confer no legal claim to a referenced asset.[13] Typically, an NFT token may be on-chain and may include metadata such as a link or URL address that refers to a reference asset.

While the token and any associated metadata for each NFT may be unique, multiple NFTs may reference an identical asset, such as the same digital image. In practice, the interchangeability of NFTs may vary based on such factors as how much the referenced asset differs substantively from those of other NFTs, and how many similar NFTs there are. For example, some NFTs have substantively unique content, as in the case of referencing

10 "Targeted Update On Implementation Of The FATF Standards On Virtual Assets And Virtual Asset Service Providers," FATF, June 2022, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf; "G20 Finance Ministers and Central Bank Governors Meetings Communique," University of Toronto, February 18, 2022, http://www.g20.utoronto.ca/2022/220218-finance.html; "A deep dive into crypto financial risks: stablecoins, DeFi and climate transition risk," European Central Bank, July 11, 2022, https://www.ecb.europa.eu/pub/financial-stability/macroprudential-bulletin/html/ecb.mpbu202207_1~750842714e.en.html.

11 "Treasury Publishes 2024 National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing," U.S. Department of the Treasury, February 2024, https://home.treasury.gov/news/press-releases/jy2080.

12 "Illicit Finance Risk Assessment of Decentralized Finance," U.S. Department of the Treasury, April 2023, https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

13 "Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art," U.S. Department of the Treasury, February 2022, https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf, 25-26; "The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067: The Role Of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets," U.S. Department of Justice, September 6, 2022, https://www.justice.gov/d9/2022-12/The%20Report%20of%20the%20Attorney%20General%20Pursuant%20to%20Section.pdf, 11.

a unique physical object, but other NFTs may be part of a large collection in which the NFTs reference content that is substantially identical despite technical differences in the token and metadata.

NFTs are managed, at least in part, through the use of self-executing code, known as smart contracts, that assign, reassign, and record ownership of each NFT. Most NFTs in the market today are created on the Ethereum blockchain,[14] or another blockchain that supports smart contracts. Since the Bitcoin blockchain lacks complex smart contracts, different technologies have been used to create NFTs using the Bitcoin blockchain.[15] There are other blockchains that are popular for or even designed specifically for NFTs.[16] Oftentimes, blockchains have specific technical standards for NFTs and related smart contracts. NFTs are usually stored through the use of digital asset wallets that are compatible with the blockchain on which the NFTs are issued.

This risk assessment is not assessing risks of all tokenized assets, only the subset of digital assets that meet the above definition for NFTs.

2.1.3 Types of NFT Platforms

NFT platforms may operate as primary markets for NFTs where an NFT is originally minted and sold, as well as secondary markets where users may exchange and re-sell previously minted NFTs, or as both, allowing individuals and entities to conduct a range of NFT creation and sale activities.[17] A small number of NFT platforms hold the majority of market share for NFT sales volumes, but there are numerous NFT platforms, some of which have a narrow focus on a specific type of NFT or specific NFT collection. NFT platforms can vary based on the characteristics below.

- ***Services Offered:*** NFT platforms may be specifically focused on providing NFT services, which could include supporting creation and sale as well as NFT lending, derivatives markets, or other activities.[18] NFT platforms may also provide other services, such as the buying and selling of broader categories of digital assets or auction services of other digital and non-digital assets.[19] The latter category may provide other services, like art galleries, or auction houses.
- ***Payment Method***: All NFT platforms allow users to purchase NFTs with virtual assets, often via stablecoins, although some platforms require users to use a platform-specific token while other platforms allow users to buy and sell through a variety of virtual assets. Some NFT platforms also allow for NFT purchases by fiat currency through third party payment processors, usually via credit or debit card.

14 Many NFTs in the market today use the ERC-721 smart contract standard, which issues one token per contract. Some NFT collections use the ERC-1155 smart contract standard, where a single smart contract may mint multiple NFTs or other tokens. When an ERC-1155 contract mints NFTs, the resulting NFTs are often similar in appearance but still maintain nominally distinguishable features. "ERC-721 Non-Fungible Token Standard," Ethereum, November 19, 2023, https://ethereum.org/en/developers/docs/standards/tokens/erc-721/; "ERC-1155 Multi-Token Standard," Ethereum, August 15, 2023, https://ethereum.org/en/developers/docs/standards/tokens/erc-1155/;

15 "An Introduction to Bitcoin NFTs," Trust Machines, n.d., https://trustmachines.co/learn/introduction-bitcoin-nfts/; NFT-like tokens called Ordinals are available on the Bitcoin blockchain, although they differ technologically from Ethereum-based NFTs, including: 1) All Ordinal content is stored on the blockchain (as opposed to off-chain content storage as detailed below); 2) Ordinals have a maximum size of four megabytes and therefore hold less content than Ethereum-based NFTs; and 3) Ordinals do not employ smart contracts for their creation or exchange; Dominic Basulto, "What Do New NFTs Mean for Bitcoin's Future Valuation?," The Motley Fool, March 6, 2023, https://www.fool.com/investing/2023/03/06/what-new-nfts-mean-for-bitcoins-future/#:~:text=After%20all%2C%20some%20forecasts%20now,billion%2C%20by%20the%20year%202030.

16 Linda Rosencrance, "Top 8 Blockchains for Developing NFTs," Techopedia, July 27, 2023, https://www.techopedia.com/top-8-blockchains-for-developing-nfts#:~:text=Ethereum,great%20for%20launching%20new%20projects.

17 See Table 2.1.1 for further information regarding NFT lifecycle.

18 In some cases, NFTs are restricted to use on a single platform.

19 "Digital Art," Sotheby's, n.d., https://www.sothebys.com/en/departments/digital-art; "Digital Art & NFTs," Christie's, n.d., https://www.christies.com/en/events/digital-art-and-nfts/overview.

- ***Sales Processes***: Some platforms allow users to buy NFTs for a set price, which may vary by the popularity of the NFT or NFT collection, while other platforms sell NFTs in auctions in which customers submit bids for a specific NFT.[20]
- ***Fees***: As with other blockchain-based transactions, NFT sales often require fees, often called gas fees, to process the transaction, which platforms often pass along to the customer. Some platforms may charge a service fee that takes a certain percentage from the buyer, the seller, or both. In some cases, platforms have optional or mandatory royalty policies, through which the original NFT creator receives a certain percentage of subsequent NFT sales. Royalties can also be built into smart contracts, which will automatically pay out the pre-determined royalty amount to the NFT creator for applicable transactions.[21]
- ***Platform Governance***: Some of the largest and most popular NFT platforms purport to be decentralized and operate through decentralized autonomous organizations[22] (DAOs) and token-based voting structures. Some platforms distribute governance tokens through reward systems such that high volume users receive governance tokens and hold greater influence over certain types of decision-making. However, this type of system can incentivize manipulative trading, such as when the buyer and seller of an NFT transaction are the same or in collusion and both parties buy or sell an NFT to artificially inflate an NFT's supposed demand and value, and lead to inflated trading volumes.

Depending on the facts and circumstances surrounding their operations, many of these platforms have AML/CFT obligations under the Bank Secrecy Act (BSA) and its implementing regulations,[23] which generally impose obligations on financial institutions and nonfinancial trades or businesses to assist U.S. government agencies in detecting and preventing money laundering, terrorist financing, and other illicit finance activity. Additionally, any NFT platform, wherever located, is generally required to comply with economic sanctions programs administered and enforced by Treasury's Office of Foreign Assets Control (OFAC) when a transaction involves a U.S. person. These obligations, as well as other regulatory obligations are explained in more detail below.

2.1.4 Types of NFTs

There are several types of NFTs designed for various purposes, including those purporting to represent ownership of physical assets, such as art, vehicles, or real estate; digital goods; or governance rights for digital asset projects and protocols. NFTs can also purport to convey other rights, such as exclusive merchandise access or VIP access at events or be used for identification and verification. This assessment reviews many of the most prominent types and uses of NFTs, although there is significant overlap among these categories. Individual NFTs may be used for different purposes over time, depending on the intentions of the NFT owner. For example, a customer may initially buy an NFT to serve as a social media profile picture, later decide to buy other NFTs within the same collection as collectibles, and choose to sell the collection for profit. Similarly, one customer could buy an NFT to display in a virtual ecosystem while a second customer could buy the same NFT with the intention of reselling it quickly as an investment product.

20 Jeff Link and Alexandria Jacobson, "Where to Buy NFTs: 20 Marketplaces and What They Sell," BuiltIn, March 31, 2023, https://builtin.com/blockchain/non-fungible-token-nft.

21 Gilbert and Hernandez, "How NFT Royalties Work," Blockworks, How NFT Royalties Work – and Sometimes Don't - Blockworks.

22 DAOs can be described as a system of administration that aspires to operate, in part, according to a set of encoded and transparent rules or smart contracts. "Illicit Finance Risk Assessment of Decentralized Finance," U.S. Department of the Treasury, April 2023, https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

23 The BSA is codified at 31 U.S.C. §§ 5311-5314, 5316-5336 and 12 U.S.C. §§ 1829b, 1951-1959. Regulations implementing the BSA are codified at 31 C.F.R. Chapter X.

Select types of NFTs are detailed below:

- ***Physical Asset Ownership:*** NFTs may purport to represent ownership of physical assets, from works of art[24] to vehicles[25] and real estate.[26] Although an NFT may purport to represent ownership of a physical asset, the owner of the relevant NFT may not hold physical custody of the physical asset represented by the NFT and may not in fact own any legal rights in the physical asset. In some cases, custody of an associated physical asset may be transferred to the NFT owner upon completion of the smart contract transaction or at a later date of the NFT owner's choosing.
- ***Ownership of Virtual Goods:*** NFTs themselves may be created and traded as individual pieces or as pieces in larger collections that share features or a theme. An NFT's value may depend on the reputation of the creator, the scarcity of items within a certain collection, or demand based on word of mouth, marketing, or social media. NFTs may not represent ownership of virtual goods like virtual trading cards;[27] virtual clothing or accessories for avatars to wear or use;[28] virtual images that can be used as avatars;[29] or virtual art.[30]
- ***Access Rights NFT:*** Some NFTs have certain benefits such as access rights associated with their ownership. Some NFTs may provide users with exclusive (digital or physical) merchandise access, VIP access at concerts or other events, and pre-sale opportunities for subsequent NFT collections.[31]
- ***Governance and Membership NFT:*** Certain DAOs within the DeFi services ecosystem as well as other projects and protocols can use NFTs as governance tokens that allow users to participate in decision-making. While many governance tokens are not currently considered NFTs, NFTs can be used to associate certain governance rights, such as decision-making authority and voting rights, to certain users. In such instances, the weight of voters could be based on the value of their NFTs.[32]
- ***Identity NFT:*** While still in nascent stages, some entities are experimenting with use of NFTs for identification and verification purposes. Because NFTs are unique and often tradeable across platforms, they could be used both online and in the real world as a form of digital identity. Some companies and individuals are researching the concept of so-called "soulbound tokens," a type of NFT that cannot be traded or transferred. Soulbound tokens therefore may have the potential to be secure, verifiable, immutable representations of individual persons and their identities.[33]

24 In 2022, an Andy Warhol piece titled "Alexander the Great" was put up for sale through pairing with an NFT, which transfers ownership of the piece of art. Janelle Borg, "Andy Warhol Artwork, Alexander the Great, to be Auctioned Off as an NFT," NFT Evening, May 4, 2022, https://nftevening.com/andy-warhol-artwork-alexander-the-great-to-be-auctioned-off-as-an-nft/.

25 In 2023, the California Department of Motor Vehicles began testing the use of NFTs representing car titles. Leo Schwartz, "California DMV puts car titles on Tezos blockchain, consumer applications on the way," Yahoo!news, January 26, 2023, https://www.yahoo.com/now/california-dmv-puts-car-titles-140000450.html.

26 In 2017, real estate and technology company Propy sold an apartment located in Kyiv, Ukraine through an NFT. Peter Grant, "An Entire Real Estate Deal Takes Place Online, Using Cryptocurrency Technology," *The Wall Street Journal*, September 26, 2017, https://www.wsj.com/articles/an-entire-real-estate-deal-takes-place-online-using-cryptocurrency-technology-1506462545.

27 Matthew DiLallo, "Investing in NFT Trading Cards," The Motley Fool, November 17, 2023, https://www.fool.com/investing/stock-market/market-sectors/financials/non-fungible-tokens/nft-trading-cards/.

28 Rachel Breia, "Wearable NFTs – Everything There's To Know About Them," Sensorium, February 13, 2022, https://sensoriumxr.com/articles/guide-to-wearable-nfts.

29 Benedict George, "What Are PFP NFTs?," CoinDesk, May 11, 2023, https://www.coindesk.com/learn/what-are-pfp-nfts/.

30 Beeple, "Everydays: The First 5000 Days," Christie's, March 11, 2021, https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924?ldp_breadcrumb=back.

31 Griffin Mcshane, "What Are Utility NFTs?," CoinDesk, March 8, 2024, https://www.coindesk.com/learn/what-are-utility-nfts/.

32 James Howell, "List of Top 10 Governance Tokens," 101 Blockchains, September 20, 2022, https://101blockchains.com/top-governance-tokens/.

33 Niall Dennehy, "Using NFTs & Soulbound Tokens to represent Digital Identity," Medium, December 28, 2022, https://medium.com/aid-tech/using-nfts-soulbound-tokens-to-represent-digital-identity-a06d63003d57.

- ***Fractional NFT:*** Because certain NFTs can cost millions of dollars, some NFT platforms and secondary markets offer users the option to purchase a portion of an NFT. The tokens created from breaking up the larger NFT can be visually unique (*e.g.*, an NFT of the 'frame' of a painting represented by the original NFT) or interchangeable (*i.e.*, virtual asset tokens issued to represent partial ownership of a specific NFT). Some platforms also offer NFT pooling, where users may deposit their NFTs, often into collection-specific pools, receive fungible tokens in return, and swap for other NFTs within the pool, making them interchangeable.

As noted in the introduction, NFTs, including the types of NFTs above, may in some cases be virtual assets, as defined by the FATF. NFTs, including those that are considered virtual assets, fall within the term digital asset, which includes virtual assets as well as other assets.

2.1.2 NFT Creation

There are several practical steps that individuals or entities typically take prior to the first sale of an NFT. NFT content design, including the creator's decisions about which assets or access rights will be associated with the token, occurs off the blockchain. Following an NFT's design, a record of the NFT is issued, or minted, on a blockchain. The minter may or may not be the same as the creator or as other roles within the NFT process. NFT metadata and the assets or access rights the token purports to represent are rarely stored on the blockchain given the expense and processing power required. However, the NFT information stored on the blockchain will often contain a URL link or other directions for how to access the NFT's referenced assets or access rights. NFTs may be stored in centralized locations like a cloud service provider or in decentralized locations such as peer-to-peer storage networks. Currently, the most popular decentralized storage platform is called the interplanetary file system (IPFS), which uses a distributed file storage protocol to store files through computers around the world on a peer-to-peer network. In some instances, both the metadata and referenced asset or access rights are only viewable to the NFT holder.

Many individuals and entities mint an NFT and post it for sale at the same time, but the two do not have to occur simultaneously. Some NFTs are minted on the blockchain but never sold; however, once an NFT is minted, the token becomes visible to the public. The keys that permit access to the off-chain NFT asset are often stored within digital asset wallets. Digital asset wallets that store an NFTs key information can use application programming interfaces (APIs) to display the NFT's content within the wallet and allow users to see not only their NFT key but also associated off-chain, stored NFT content. Select roles and processes in NFT are described in table 2.1.1; note that the roles can be executed by the same or different persons.

Table 2.1.1 NFT Creation Process

Role	Activities
Creator	Designs appearance or content of NFT, typically in a digital format such as a JPEG, PNG, or GIF.
Minter	Deploys/executes code such that NFT data are placed on the blockchain, usually done by uploading the NFT file to a digital asset wallet, connecting the wallet to an NFT platform, and choosing on which blockchain the NFT will be placed.
Issuer	Conducts primary offer and sale of NFT, once uploaded to a blockchain, and can include an NFT platform.
Redeemer	Enables redemption of an NFT that purports to be redeemable for a referenced asset.

While creators can mint and issue a single NFT, many choose to mint and issue entire NFT collections at once. Limited edition NFT collections contain a specific number of NFTs, where only a predetermined amount can be minted. This scarcity is intended to increase the value of each NFT within that collection. Most NFT collections are limited edition, although some NFT collections have been minted and placed for sale and issued through an open edition process.[34] Open edition NFT collections allow for an unlimited number of NFTs to be minted by collectors or members of an NFT collection community. However, the administrator of the collection will often set a time limit on the minting period (usually 24-72 hours) during which the NFTs must be minted. Open edition NFT collections are usually cheaper given the lack of scarcity, but prices can rise after a minting period closes. Open edition NFT collections use the ERC-1155 smart contract standard. Limited edition NFT collections often use the ERC-721 smart contract standard.

2.2 Market Overview

Since the creation of the first NFT in 2014[35] and the introduction of NFTs to the Ethereum blockchain in 2017, NFT sales and trading volumes have fluctuated significantly. It can be difficult to determine the true total value of the NFT market given the prevalence of manipulative trading tactics, which artificially inflates transaction values and volumes. Industry analysis on the total market value for NTFs varies widely, possibly as a result of some analysis attempting to exclude wash trading and making choices as to which NFTs are being tracked in the analysis.[36] Moreover, sales and trading volumes for NFTs vary from month to month as new products and services receive attention upon launch but often decrease in popularity after a short time. In broad trends, the NFT market grew immensely in the summer of 2021, and NFT sales peaked in early-to-mid 2022 before decreasing sharply through the end of 2022.[37] In 2023, NFT trading volumes increased early in the year, partially attributed to the rise of a new NFT marketplace and the introduction of Bitcoin Ordinals, before dipping back down.[38] As an illustration, one analytics company identified that Ethereum NFT marketplace monthly volumes, filtered for wash trading, peaked at $5.36 billion in January 2022 before falling to just over $240 million in September 2023; the volume for March 2024 was nearly $800 million.[39] Other industry sources support these trends, with one industry report finding that transaction volume and average NFT prices fell in 2023 compared to 2022,[40] and another highlighting that NFT sales in the third quarter of 2023 were the lowest in three years.[41]

34 Joel Agbo, "Open Edition vs. Limited Edition NFTs," CoinGecko, February 16, 2023, https://www.coingecko.com/learn/open-edition-nft-vs-limited-edition-nft.

35 The first NFT, "Quantum," was minted in 2014 on the Namecoin blockchain. The NFT is a digital artwork with pulsating color in an octagon against a black background. MK Manoylov, "A brief history of NFTs: From CryptoPunks to Bored Apes," The Block, October 18, 2023, https://www.theblock.co/learn/251477/a-brief-history-of-nfts.

36 "Highest Price NFT Stats," CoinMarketCap, accessed February 25, 2024, https://coinmarketcap.com/nft/; "NFT Market Report for January 2024: Your Guide to Understanding & Investing," CoinPedia, February 2, 2024, https://coinpedia.org/research-report/nft-market-monthly-report-january-2024-analysis-and-insights/; "NFT Collection Prices & Charts Today by Trading Volume," *Forbes*, accessed February 25, 2024, https://www.forbes.com/digital-assets/nft-prices/?sh=5cd246546dfb; "NFT stats overview," OKX, accessed February 25, 2024, https://www.okx.com/web3/marketplace/nft/stats/overview.

37 Andrew Hayward, "NFT Sales in 2022 Nearly Matched the 2021 Boom, Despite Market Crash," Decrypt, January 4, 2023, https://decrypt.co/118438/2022-versus-2021-nft-sales; "NFTs and Financial Crime," Elliptic, August 24, 2022, https://www.elliptic.co/resources/nfts-financial-crime.

38 NFTGo, "2023 NFT Market Analysis: An Insider Look," CoinMarketCap, May 2023, https://coinmarketcap.com/academy/article/2023-nft-market-analysis:-an-insider-look.

39 Ethereum NFT Marketplace Monthly Volume (theblock.co)

40 Julius Mutunkei, "NFT market analysis: 2023 highlights and 2024 forecast," Crypto.news, December 30, 2023, https://crypto.news/nft-market-analysis-and-forecast/.

41 Mandy Williams, "Q3 2023 Was the Worst Quarter for NFT Sales in 3 Years: Report," CryptoPotato, October 23, 2023, https://cryptopotato.com/q3-2023-was-the-worst-quarter-for-nft-sales-in-3-years-report/.

NFTs account for a relatively small portion of overall market value of digital assets, likely no more than 10 percent using high estimates of NFT total market value.[42]

3. Illicit Finance Threats

As stated in the 2024 Illicit Finance Strategy and the 2024 NRAs, most money laundering, terrorist financing, and proliferation financing by volume and value of transactions occurs using fiat currency.[43] The assessment identifies that NFTs and NFT platforms are rarely, if at all, being used for drug trafficking, proliferation financing, or terrorist financing. However, it does find that NFTs are susceptible to use in fraud and scams, many of which are traditional schemes that involve NFTs, and can be stolen from victims. Additionally, criminals use NFTs to launder proceeds from predicate crimes often in combination with other techniques or transactions meant to obfuscate the illicit source of funds. While not fully explored in this assessment, some threat actors, like drug traffickers, are increasingly using virtual assets, which could potentially evolve into increasing use of NFTs. Still, there is limited information on misuse of NFTs for these and other types of illicit activity, like sanctions evasion, other than limited targeting for theft by DPRK cybercriminals.

This risk assessment draws on case examples Treasury identified and analyzed in its research and consultations with law enforcement, regulators, and other U.S. government stakeholders. However, final adjudication often takes years to complete. Given how recent and ongoing the evolution of the NFT market is, there were relatively few case examples that this assessment could include. This does not, however, necessarily reflect the level of risk.

In preparation of this assessment, Treasury extensively reviewed open-source information, including media and industry reports analysis. The risk assessment was also informed by consultations with several U.S. government departments and agencies and the over 75 responses to Treasury's Request for Comment, which was issued in conjunction with the publication of the Action Plan.

3.1 Money Laundering

Thieves, scammers, and other bad actors have used a variety of techniques to transfer and launder illicit proceeds using NFTs and NFT platforms, including self-laundering, rapid sales, and the use of multiple NFT platforms. Criminals often try to sell or trade stolen or illicitly-gained NFTs quickly in order to evade discovery, obfuscate the source of NFTs, or complicate the ability of NFT platforms, blockchain analytics companies, and law enforcement to trace the location of the NFTs and any profits from illicit sales. Additionally, law enforcement has observed that illicit actors often take advantage of the fact that many NFT platforms do not require customer information. The techniques can be enabled by the ability to send or receive NFTs across borders, nearly instantaneously, like many other digital assets; many NFT platforms lack controls to identify customers or otherwise mitigate illicit finance risks; and other vulnerabilities outlined in Section 4.

42 "Highest Price NFT Stats," CoinMarketCap, accessed February 25, 2024, https://coinmarketcap.com/nft/; "NFT Market Report for January 2024: Your Guide to Understanding & Investing," CoinPedia, February 2, 2024, https://coinpedia.org/research-report/nft-market-monthly-report-january-2024-analysis-and-insights/; "NFT. Collection Prices & Charts Today by Trading Volume," *Forbes*, accessed February 25, 2024, https://www.forbes.com/digital-assets/nft-prices/?sh=5cd246546dfb; "NFT stats overview," OKX, accessed February 25, 2024, https://www.okx.com/web3/marketplace/nft/stats/overview.

43 "Treasury Publishes 2024 National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing," U.S. Department of the Treasury, February 2024, https://home.treasury.gov/news/press-releases/jy2080; "Treasury Announces 2024 National Illicit Finance Strategy," U.S. Department of the Treasury, May 2024, https://home.treasury.gov/news/press-releases/jy2346.

Laundering techniques involving NFTs include:

- ***Self-Laundering:*** Self-laundering is a variation of manipulative trading (*see* section 3.1.1) in which illicit actors purchase an NFT with illicit funds and sell the NFT to themselves using a different digital wallet to create records of sale on the blockchain. The NFT can then be sold to unwitting victims and may compensate criminals with clean funds not tied to a prior crime.[44]
- ***Layering:*** The highly automated nature of NFT sales and wide availability of NFTs across different NFT platforms provide illicit actors with the ability to buy and sell NFTs quickly, whether following the theft of an NFT or in order to create additional 'hops' for laundering assets. In some instances, criminals will prioritize speed over profits, selling NFTs at a loss in the process. Rapid transactions can complicate blockchain analysis and transaction tracing. Once the criminals have purchased and sold several NFTs, they may launder virtual asset proceeds using mixers, such as Tornado Cash as identified by one industry report in 2022,[45] or use other obfuscation techniques before exchanging virtual assets for fiat currency. Tornado Cash was designated by OFAC in August 2022 and redesignated by OFAC under separate authorities in November 2022.[46] Illicit actors may also buy or sell NFTs in a manner that may be perceived as for consumption or investment purposes to conceal illicit payments which can be supported by the fluctuating value of NFTs.
- ***Use of Multiple NFT Platforms or Accounts:*** Criminals may use multiple platforms or hold multiple accounts at the same platform to conduct their activity to insulate against their accounts being detected and deactivated. For example, they could buy or steal an NFT through one platform and sell the same NFT on a different platform.

In addition to using NFTs and NFT platforms in the laundering process, illicit actors may also use NFTs to generate funds, using some of the methods identified below.

3.1.1 Investment Fraud and Scams

The NFT market is particularly vulnerable to fraud and scams. According to a blockchain analytics firm, over $100 million worth of NFTs were stolen through scams between July 2021 and July 2022.[47] According to the same report, in May 2022, just under $24 million worth of NFTs were stolen through scams. These numbers likely understate the total because victims of theft and scams often do not publicly report their losses. Criminal actors employ a range of techniques, outlined below, most of which mimic traditional scams and/or involve conflicts of interest, while others are unique to NFTs and NFT platforms.

- ***Rug Pulls:*** In a rug pull, a scammer raises investment funds in a seemingly legitimate project, such as an NFT collection, before ending the project and stealing invested funds. Recently, law enforcement has noted an increase in 'slow rug pulls' in which criminals use the proceeds of one fraudulent NFT project to fund a second NFT project or collection while remaining in contact and continuing to make promises to the victims of the original project.
- ***Market Manipulation:*** Criminals may engage in price manipulation by engaging in intentional or willful conduct designed to deceive or defraud investors. One type of price manipulation includes wash trading. Some research suggests that wash trading occurs frequently within the NFT market, with one study concluding that 58 percent of Ethereum-based NFT trades in 2022 were associated with wash trading.[48] In total, over $30 billion in NFT trading volume may be linked to wash trading according to the same study.

44 "Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art," U.S. Department of the Treasury, February 2022, https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf.

45 "NFTs and Financial Crime," Elliptic, August 24, 2022, https://www.elliptic.co/resources/nfts-financial-crime.

46 "Treasury Designates DPRK Weapons Representatives," U.S. Department of the Treasury, November 8, 2022, https://home.treasury.gov/news/press-releases/jy1087.

47 "NFTs and Financial Crime," Elliptic, August 24, 2022, https://www.elliptic.co/resources/nfts-financial-crime.

48 Rosie Perper, "Over $30B of NFT Trading Volume on Ethereum Is Wash Trading, Research Suggests," CoinDesk, December 23, 2022, https://www.coindesk.com/web3/2022/12/23/over-30b-of-nft-trading-volume-on-ethereum-is-wash-trading-research-suggests/.

- ***Fake and Counterfeit Sales:*** Some scammers create NFTs that purport to be part of rare, popular, and expensive NFT collections, or associated with existing brands but are in fact counterfeits and unrelated to genuine NFT collections or identified brands. Other scammers may mint NFTs that are unauthorized copies of copyrighted works, including popular images or artwork, or misrepresent the assets or access rights, or rights associated with the NFT, that purportedly were conveyed with the token. In a particular form of counterfeiting called "sleepminting," a hacker can mint an NFT to appear as if it was minted by a legitimate NFT creator and may try to sell the counterfeit NFT at a price comparable to the legitimate creator's work.
- ***Fraudulent NFT Platforms:*** Scammers may renege on agreements to exchange NFTs with other platform users or may create their own fraudulent platforms to steal users' NFTs. In one instance, the creators of a purported NFT platform used smart contracts to steal high-value NFTs totaling approximately $200,000 in value and laundered the funds using the Tornado Cash mixer.[49]
- ***Conflicts of Interest:*** Persons with access to confidential information related to NFT platforms may use advanced knowledge of promotions or other market activity for their own financial gain. This includes cases of illegal insider trading, which refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, on the basis of material, nonpublic information about the security.
- ***Chargeback Scams:*** Scammers use credit cards to purchase NFTs from an NFT platform and send the NFT to a digital asset wallet. They then dispute the transaction with their credit card company, claiming that they did not authorize the transaction and do not own the wallet to which the NFT was sent and request reimbursement.[50]

Case Examples

- In August 2023, Nathaniel Chastain, a former product manager at the NFT platform OpenSea, was sentenced to three months in prison in connection with a scheme to commit insider trading in NFTs, by using confidential information about which NFTs were going to be featured on OpenSea's homepage for his personal financial gain. Chastain was convicted of related wire fraud and money laundering offenses.[51] According to the Justice Department, to conceal the fraud, Chastain used anonymous OpenSea accounts to make purchases and sales and transferred funds through multiple anonymous Ethereum accounts in order to conceal his involvement in purchasing and selling NFTs.[52] Chastain used new Ethereum accounts without any prior transaction history.
- In January 2023, the Department of Justice (DOJ), DHS-ICE Homeland Security Investigations (HSI), and Internal Revenue Service-Criminal Investigation (IRS-CI) charged Aurelien Michel with defrauding purchasers of "Mutant Ape Planet" NFTs of more than $2.9 million in virtual assets. As alleged, Michel perpetrated a rug pull scheme—stealing nearly $3 million from investors for his own personal use. As part of the scheme, NFTs were marketed to purchasers, who were falsely promised numerous rewards and benefits designed to increase demand for, and the value of, their newly acquired NFTs. Once the NFTs were sold out, Michel allegedly ceased communications and withdrew purchasers' funds from the company's virtual asset wallets for his own personal benefit.[53]

49 "NFTs and Financial Crime," Elliptic, August 24, 2022, https://www.elliptic.co/resources/nfts-financial-crime.

50 "NFT Chargeback Exclusion Points to Growing Concerns Over Fraud," PYMNTS, February 16, 2022, https://www.pymnts.com/news/security-and-risk/2022/nft-chargeback-exclusion-points-growing-concerns-over-fraud/.

51 "Former Employee Of NFT Marketplace Sentenced To Prison In First-Ever Digital Asset Insider Trading Scheme," U.S. Department of Justice, August 22, 2023, https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-sentenced-prison-first-ever-digital-asset-insider.

52 "Nathaniel Chastain Indictment," U.S. Department of Justice, June 1, 2022, https://www.justice.gov/d9/press-releases/attachments/2022/06/01/u.s._v._nathaniel_chastain_indictment.pdf.

53 "Non-Fungible Token (NFT) Developer Charged in Multi-Million Dollar International Fraud Scheme," U.S. Department of Justice, January 5, 2023, https://www.justice.gov/usao-edny/pr/non-fungible-token-nft-developer-charged-multi-million-dollar-international-fraud.

- In June 2022, DOJ and law enforcement partners announced that Le Anh Tuan was charged with one count of conspiracy to commit wire fraud and one count of conspiracy to commit international money laundering in the U.S. District Court for the Central District of California in connection with a scheme involving the "Baller Ape" NFT.[54] Tuan allegedly was involved in the Baller Ape Club, an NFT investment project that purportedly sold NFTs in the form of various cartoon figures, often including the figure of an ape. According to the indictment, shortly after the first day Baller Ape Club NFTs were publicly sold, Tuan and his co-conspirators engaged in a rug pull, ending the purported investment project, deleting its website, and stealing the investors' money. In total, Tuan and his co-conspirators allegedly obtained approximately $2.6 million from investors.

3.1.2 Theft

NFTs are vulnerable to theft through malware, exploitation of vulnerabilities in smart contracts, and other deceptive practices. Many thieves do not differentiate between virtual assets and NFTs and may inadvertently steal NFTs.

- ***Malware:*** Illicit actors spread malware that drains victims' digital asset wallets through malicious links to social media, purported advertisements by known industry participants, or NFTs airdropped into user digital asset wallets.[5556] In some instances, illicit actors either gain direct access to NFT developer social media accounts or create almost identical accounts to promote new NFT releases. Links provided in these announcements are phishing links directing victims to a spoofed website that appears to be a legitimate extension of a particular NFT project. The spoofed websites invite victims to connect their digital asset wallets and purchase the NFT. The victims unknowingly connect their digital asset wallets to a drainer smart contract, resulting in the transfer of digital asset and NFTs to wallets operated by criminals. For example, in April 2022, criminals hacked into and took over the social media account of a prominent NFT collection creator and shared links to a website the criminals then used to steal NFTs worth over $40 million.[57] In another example, hackers airdropped NFTs that purported to contain software updates from a digital asset wallet. The airdropped NFTs included malware that prompted users to download an update, which stole user information, including wallet credentials.[58]
- ***Smart Contract Exploitation:*** Illicit actors have exploited bugs and other vulnerabilities within smart contracts to steal NFTs and purchase rare NFTs at highly reduced prices. Because smart contracts are in some cases immutable, in many cases developers are unable to fix or rescue funds from smart contract exploits and hacks. In one instance, a hacker discovered a bug in an NFT smart contract that enabled them to begin and cancel purchases of an NFT until they received an NFT with favorable, rare characteristics and metadata valued at approximately $700,000.[59]

54 "Justice Department Announces Enforcement Action Charging Six Individuals with Cryptocurrency Fraud Offenses in Cases Involving Over $100 Million in Intended Losses," U.S. Department of Justice, June 30, 2022, https://www.justice.gov/opa/pr/justice-department-announces-enforcement-action-charging-six-individuals-cryptocurrency-fraud.

55 Jesse Coghlan, "Google Ads-delivered malware drains NFT influencer's entire crypto wallet," Cointelegraph, January 16, 2023, https://cointelegraph.com/news/google-ads-delivered-malware-drains-nft-influencer-s-entire-crypto-wallet.

56 "Criminals Pose as Non-Fungible Token (NFT) Developers to Target Internet Users with an Interest in NFT Acquisition," Federal Bureau of Investigation, August 4, 2023, https://www.ic3.gov/Media/Y2023/PSA230804.

57 Zhiyuan Sun, "Bored Ape Yacht Club NFTs stolen in Instagram phishing attack," Cointelegraph, April 25, 2022, https://cointelegraph.com/news/bored-ape-yacht-club-nfts-stolen-in-instagram-phishing-attack.

58 Lawrence Abrams, *Fake Solana Phantom security updates push crypto-stealing malware*, Bleeping Computer, (October 9, 2022), https://www.bleepingcomputer.com/news/security/fake-solana-phantom-security-updates-push-crypto-stealing-malware/.

59 Andrew Thurman, "$85 million 'Meetbits' NFT project exploited; attacker nabs $700,000 collectible," Cointelegraph, May 8, 2021, https://cointelegraph.com/news/85-million-meebits-nft-project-exploited-attacker-nabs-700-000-collectible.

3.2 Proliferation Finance

Under pressure from robust U.S. and UN sanctions, the Democratic People's Republic of Korea (DPRK) has resorted to illicit activities, including cyber-enabled thefts from VASPs and other financial institutions, to generate revenue for its unlawful weapons of mass destruction (WMD) and ballistic missile programs.[60] DPRK cyber actors in 2022 raised more than $720 million from virtual asset heists against virtual asset projects and firms, accounting for the vast majority of Pyongyang's revenue generated through cybercrime. A U.S. cybersecurity firm separately identified an NFT theft scheme they attributed to DPRK cyber actors in 2022, although proceeds from this NFT scheme likely account for a very small portion of overall DPRK cyber-enabled digital asset theft.[61] The cybersecurity firm detailed how DPRK cyber actors allegedly used nearly 500 decoy websites designed to look like NFT products to socially engineer victims to expose their private keys by visiting malicious websites, allowing the cyber actors to steal their NFT holdings. One of these decoys was able to steal over 1,000 NFTs and subsequently converted them into Ether worth over $350,000 and sent the funds to VASPs and other virtual asset wallet addresses, according to the cybersecurity firm.

In addition to stealing funds from virtual asset firms and projects, DPRK-linked actors have engaged in separate activities within the digital asset ecosystem that indicate that the group may have the expertise and access to increasingly abuse NFTs to generate revenue. For example, the DPRK has dispatched thousands of highly skilled information technology (IT) workers around the world who often are employed to work on projects involving digital assets.[62]

3.3 Terrorist Financing

While there is potential for terrorist groups to use NFTs to raise or move funds, the few examples of this occurring in practice indicate that efforts to raise funds using NFTs have not been successful. Treasury's 2024 National Terrorist Financing Risk Assessment found that terrorist financing activity in the United States has evolved but that groups largely continue to employ established methods for raising and moving funds.[63] In particular, terrorist groups commonly use money services businesses, in particular outside of the United States where financial institutions are less subject to regulatory oversight, and unregulated cash-based networks to transfer funds. They may use a variety of methods, including kidnapping for ransom, looting, taxation, legal commercial activities, donations, and self-financing to fund their activities. The assessment recognized, however, that some terrorist groups, including the Islamic State of Iraq and Syria (ISIS), Al-Qa'ida, Hamas, and domestic violent extremist (DVE) groups, have demonstrated an ability to adapt to use new technologies. Private sector reports indicate that some pro-Russian Racially and Ethnically Motivated Violent Extremist (REMVE) groups may be starting to use NFTs in fundraising (see Text Box 1), although the U.S. government does not have any cases with these or other terrorist groups using NFTs for these purposes.

60 "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats," U.S. Department of the Treasury, May 6, 2022, https://home.treasury.gov/news/press-releases/jy0768.

61 SlowMist, SlowMist: Investigation of North Korean APT's Large-Scale Phishing Attack on NFT Users, (December 24, 2022), https://slowmist.medium.com/slowmist-our-in-depth-investigation-of-north-korean-apts-large-scale-phishing-attack-on-nft-users-362117600519.

62 U.S. Department of the Treasury, U.S. Department of State, Federal Bureau of Investigation,, "Guidance on the Democratic People's Republic of Korea Information Technology Workers," U.S. Department of the Treasury, May 16, 2022, https://ofac.treasury.gov/media/923126/download?inline.

63 "2024 National Terrorist Financing Risk Assessment," U.S. Department of the Treasury, February, 2024, https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf.

NFTs and the Further Russian Invasion of Ukraine

Pro-Russian organizations abroad, including REMVE organizations and entities designated by the United States as Specially Designated Global Terrorist, may be using NFTs, NFT collections, and NFT platforms to raise funds for Russian and Russian-affiliated soldiers fighting in Ukraine. One such project, the Terricon Project, was created in April 2022 in order to raise funds while circumventing U.S. sanctions, according to the project's website.[64] The Terricon Project website also advertised the sale of several NFTs depicting pro-Russian stances on the OpenSea NFT marketplace. The collection was deleted from OpenSea's website prior to the completion of any sales, but the data behind the collection remains on the blockchain.[65] Telegram channels associated with Russia paramilitary organization the Wagner Group have also encouraged the purchase of NFTs for investment purposes.[66]

NFTs may also offer extremist groups a method for spreading messaging. For example, in 2022, an NFT was minted to an NFT trading website bearing the Islamic State of Iraq and Syria (ISIS) emblem by a supporter of the group who also minted two other NFTs exhibiting ISIS hallmarks.[67] There were no indications that the NFTs were part of a broader ISIS effort, but they did demonstrate that terrorist groups could potentially use NFTs for messaging purposes. While NFT platforms are able to remove listed NFTs for sale on their platform, NFT data on the blockchain will remain viewable and the NFTs content may also remain accessible. Terrorist propaganda using NFTs, however, has not been widely observed, in particular compared to more traditional messaging efforts, such as social media and dedicated online news outlets.

4. Vulnerabilities

There are certain vulnerabilities related to the nature and technologies of NFTs, the assets or entitlements that they reference or purport to convey, and the regulatory and enforcement frameworks in the United States and abroad that can enable their misuse by illicit actors. In particular, criminals exploit cyber-related vulnerabilities, challenges with trademark and copyright protections related to NFTs, and hype and fluctuating pricing of NFTs to perpetrate crimes related to NFTs. Moreover, NFT industry non-compliance with applicable regulations in the United States and gaps in AML/CFT or other regulatory obligations for foreign-based NFT platforms can also present vulnerabilities. There may be opportunities to provide additional clarity with regards to the application of different regulatory obligations to NFT platforms to increase compliance by the industry.

4.1 Cyber-Related Vulnerabilities

NFT platforms and projects, as part of the digital asset ecosystem, operate in a market without binding or normative requirements for cybersecurity. In particular, the smart contracts that mint NFTs, dictate certain characteristics, and transfer ownership are vulnerable to hacks and other cyber exploits.

64 Nick Grothaus, Robert Kim, Kharon Staff, "NFT Sale Linked to Sanctioned Russian Terrorist Group Attempts to Support War in Ukraine," Kharon, July 14, 2022, https://www.kharon.com/updates/nft-sale-linked-to-sanctioned-russian-terrorist-group-attempts-to-support-war-in-ukraine.

65 "Crypto in Conflict," Elliptic, March 17, 2023, https://www.elliptic.co/hubfs/Elliptic_Crypto_in_Conflict_Report.pdf?hsCtaTracking=606229a1-8a8e-41af-9df1-66e8290f007c%7C331ca66d-ef91-4a94-93ed-fa010206a959, 68.

66 "Crypto in Conflict," Elliptic, March 17, 2023, https://www.elliptic.co/hubfs/Elliptic_Crypto_in_Conflict_Report.pdf?hsCtaTracking=606229a1-8a8e-41af-9df1-66e8290f007c%7C331ca66d-ef91-4a94-93ed-fa010206a959.

67 Ian Talley, "Islamic State Turns to NFTs to Spread Terror Message," *The Wall Street Journal*, September 6, 2022, https://www.wsj.com/articles/islamic-state-turns-to-nfts-to-spread-terror-message-11662292800.

Many NFT creators make their code viewable to the public, which can increase transparency and users' interest in subsequent NFTs and NFT collections. This can also, however, provide opportunities for cybercriminals to review the code and identify potential exploits to enable theft or other misuses.[68] Vulnerabilities in smart contracts could be compounded by the limited number of developers working on blockchain protocols, the re-use of code for various projects, the potential for criminals to purposefully design smart contracts with back-doors, and the lack of external oversight or formal self-regulation for code "audits."[69] Code audit firms may or may not have the requisite expertise to audit any particular blockchain protocol, and protocols "crowdsource" audits through "bug bounty" programs that offer rewards for good citizens who report flaws.

In addition to exploiting vulnerabilities within NFT platforms and projects, NFT firms are potentially at risk for software and hardware vulnerabilities commonly exploited by malicious actors across all business types, in addition to vulnerabilities specific to NFT and other digital asset firms. For example, criminals have used phishing techniques by compromising social media or email accounts of NFT platforms or projects to distribute malware to victims. In some cases, the malware is designed to steal information, in particular wallet credentials, enabling the theft of NFTs.

4.2 Copyright and Trademark Protection

Criminals may misrepresent the actual rights, particularly to an NFT's referenced asset or access right, that an NFT might actually convey. Criminals may also violate copyright and trademark protections to market NFTs. These tactics could inflate the price of an NFT. Many NFT platforms rely on individual platform users or intellectual property owners to identify copyright or trademark infringements affecting their works or brands, and screening can be resource-intensive and expensive. Additionally, NFT marketplaces may not require sellers to provide real names, making it difficult to identify infringers, and some persons responsible may be located outside of the United States, raising jurisdictional challenges.

Moreover, given disclosure and integrity gaps, consumers can unknowingly buy an NFT associated with infringing material. This can be complicated by consumer confusion about the rights conveyed with NFTs, which are often unclear or non-existent and can vary across platforms and by NFT.[70] NFT markets can be exploited by illicit actors who may fraudulently promise physical ownership or intellectual property rights of referenced assets or access rights represented by an NFT, develop and sell counterfeit NFTs, or employ similar techniques.

4.3 Hype and Fluctuating Pricing

The value of NFTs may fluctuate based on rapidly changing trends, demand, and scarcity, among other reasons. Criminals have taken advantage of the quick-moving nature of the market, in particular exploiting the publicity and hype surrounding NFTs. In some instances, scammers will indicate that fraudulent offers are time-sensitive or indicate that potential victims have early and unique access to rare NFT collections. Such tactics increase pressure on victims to act quickly to avoid missing potentially lucrative opportunities. The fluctuating pricing of NFTs can also increase pressure for victims to act quickly in the hopes that an NFT's value increases after their purchase.

68 "The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067," 10.

69 Generally, a smart contract audit is a term used by participants to describe a voluntary method for offering assurances about a DeFi arrangement's code. Participants may be offering these types of assessments to provide investors or users assurances in a particular DeFi arrangement's legitimacy, functionality, governance mechanisms, cybersecurity, and other features. However, while a smart contract audit may be useful in identifying potential vulnerabilities in specific smart contracts, protocols, or blockchain networks, these types of services in practice may not provide meaningful assurances to investors and users, "Final Report with Policy Recommendations for Decentralized Finance," The Board of the International Organization of Securities Commissions, December 2023, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf.

70 "Crypto-Assets: Implications for Consumers, Investors, and Businesses," U.S. Department of the Treasury, September, 2022, https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf.

The fluctuating nature of NFT pricing also creates vulnerabilities, as it may be difficult to determine whether an NFT is priced appropriately or is part of price manipulation, money laundering, or other illicit finance schemes. While the average price for an NFT dropped sharply in September 2023 to $38.17, from an August 2021 peak of $791.84, according to one industry report, many NFTs have sold and continue to sell for hundreds of thousands, or even millions, of dollars' worth of virtual assets.[71] Criminals may also easily inflate or reduce the price of certain NFTs to hide the exchange of illegitimate funds. This vulnerability is similar to the use of other items that sell at high-value such as art to launder illicit proceeds, although the vulnerabilities may be greater in NFTs due to the ability to move NFTs over the blockchain without physical constraints relevant in the traditional art market.

4.4 Non-Compliant NFT Platforms, Varying Interpretations of U.S. Regulatory Obligations

Regulatory obligations for service providers in in the United States, including related to the BSA and its implementing regulations, are generally activities-based and do not depend on what a platform calls itself or how it describes the services it offers. The applicable regulatory, supervisory, and enforcement framework is generally based on the product or service provided and whether an activity is covered by a civil or criminal statute. The U.S. regulatory approach is technology-neutral. Regulators have clarified this general approach in public statements and guidance and have taken enforcement actions that have dealt specifically with NFTs. Notwithstanding such clarification, some NFT industry participants have claimed not to understand or not be subject to their obligations, including related to AML/CFT, investor protection, and market integrity.

4.4.1 AML/CFT and Sanctions Obligations

NFT platforms, depending on the types of activities they facilitate, may qualify as financial institutions under the BSA and therefore have AML/CFT obligations. Whether an entity falls under the BSA's definition of "financial institution" depends on the specific facts and circumstances of the activity, rather than a label an actor affixes to that activity.[72] Thus, whether an NFT-affiliated actor is subject to the BSA would depend, for example, on the function of the NFTs offered, rather than terminology or marketing terms that the platform applies. Additionally, platforms or other persons doing business transferring virtual assets, which as noted above can include NFTs, may have U.S. AML/CFT obligations under FinCEN's rules for money service businesses if they are doing business wholly or in substantial part, in the United States.[73] NFT platforms that are financial institutions for the purposes of the BSA have the attendant AML/CFT obligations, including the requirement to establish and maintain an AML program and comply with applicable transaction monitoring, recordkeeping, and reporting requirements (including the filing of suspicious activity reports).

Where an NFT platform does not comply with its BSA obligations, there is risk that the activity will further illicit finance activity. Similarly, to the extent an NFT platform operates under the erroneous belief that it falls outside the BSA, a vulnerability may exist due to the reduced likelihood that such NFT platforms would choose to implement AML/CFT measures. Such entities may, however, still be subject to other enforcement authorities or legal requirements that could mitigate harm to the financial system or consumers.

Any NFT platform, wherever located, is generally required to comply with economic sanctions programs administered and enforced by OFAC when a transaction involves a U.S. person. When entities with relevant obligations fail to register with the appropriate regulator, fail to establish and maintain sufficient AML/CFT

71 Mandy Williams, "Q3 2023 Was the Worst Quarter for NFT Sales in 3 Years: Report," CryptoPotato, October 23, 2023, https://cryptopotato.com/q3-2023-was-the-worst-quarter-for-nft-sales-in-3-years-report/.

72 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).

73 31 C.FR. § 1010.100(ff)(5)(i)(A) (2024), "FinCEN Guidance," FinCEN, May 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

controls, or do not comply with sanctions obligations, criminals are more likely to exploit their services successfully, including to circumvent U.S. and UN sanctions.

4.4.2 Investor Protection and Market Integrity Obligations

Certain financial institutions in the United States are subject to statutes and regulations that create a robust investor protection and market integrity regime, providing for disclosures to investors that include material information to understand the risks of participation and to make more informed decisions regarding their investments, among other protections. Depending on activities in which an NFT platform or issuer may be engaged, they may be subject to these statutes and regulations, including but not limited to obligations to register. For example, depending on the facts and circumstances, an NFT could be offered and sold as a security subject to the federal securities issuers, securities intermediaries, or both laws. However, some digital asset firms may view themselves—and thus operate as if—their digital asset activities are not subject to federal laws and regulations. As a result, such firms may be acting in non-compliance and, thus, do not maintain adequate protocols to protect the public and the U.S. financial system.

- In August 2023, the SEC charged Impact Theory, LLC, a media and entertainment company headquartered in Los Angeles, California, with conducting an unregistered offering of crypto asset securities in the form of purported NFTs.[74] According to the SEC's order, from October to December 2021, Impact Theory offered and sold three tiers of NFTs, known as Founder's Keys. The order finds that Impact Theory encouraged potential investors to view the purchase of a Founder's Key as an investment into the business, stating that investors would profit from their purchases if Impact Theory was successful in its efforts. Without admitting or denying the SEC's findings, Impact Theory agreed to a cease-and-desist order finding that it violated registration provisions of the Securities Act of 1933 and ordering it to pay a combined total of more than $6.1 million in disgorgement, prejudgment interest, and a civil penalty.[75]
- In September 2023, the SEC charged Stoner Cats 2 LLC (SC2) with conducting an unregistered offering of crypto asset securities in the form of purported NFTs that raised approximately $8 million from investors to finance an animated web series called Stoner Cats.[76] According to the SEC's order, SC2 violated the Securities Act of 1933 by offering and selling these crypto asset securities to the public in an unregistered offering that was not exempt from registration. Without admitting or denying the SEC's findings, SC2 agreed to a cease-and-desist order and to pay a civil penalty of $1 million.[77]

74 "SEC Charges LA-Based Media and Entertainment Co. Impact Theory for Unregistered Offering of NFTs," Securities and Exchange Commission, August 28, 2023, https://www.sec.gov/news/press-release/2023-163.

75 SEC, Cease-and-Desist Order, "In the Matter of IMPACT THEORY, LLC," https://www.sec.gov/files/litigation/admin/2023/33-11226.pdf.

76 "SEC Charges Creator of Stoner Cats Web Series for Unregistered Offering of NFTs," Securities and Exchange Commission, September 13, 2023, https://www.sec.gov/news/press-release/2023-178.

77 SEC, "Cease-and-Desist Order In the Matter of STONER CATS 2, LLC,," https://www.sec.gov/files/litigation/admin/2023/33-11233.pdf.

4.4.3 Uneven Application of AML/CFT Obligations in Foreign Jurisdictions

Few other countries have issued regulatory guidance or taken enforcement actions related to NFTs and NFT platforms.[78] The FATF's 2019 Updated Guidance for a Risk Based Approach to Virtual Assets and VASPs indicated that some NFTs may be considered virtual assets, in which case NFT platforms offering those virtual assets should have AML/CFT obligations. The guidance, however, does not provide specific examples of which types of NFTs would constitute virtual assets compared to which would not. Many jurisdictions have indicated that they take an activities-based approach to regulation, finding that an NFT service provider could have AML/CFT obligations as VASPs if the NFTs are considered virtual assets or as financial institution types depending on the services provided.

Even for cases in which jurisdictions determine that NFT service providers are VASPs, jurisdictions may lack sufficient supervision and monitoring systems to effectively conduct supervision and sanction non-compliant VASPs, according to a June 2023 FATF report based on a voluntary survey of jurisdictions.[79] Moreover, the report found that one-third of countries have not yet completed an illicit finance risk assessment for virtual assets and over 40 jurisdictions had not decided if and how to regulate the virtual asset sector for AML/CFT purposes. Similarly, many jurisdictions have not determined an approach to NFTs. This indicates that many jurisdictions have not yet considered or taken steps to mitigate illicit finance risks associated with NFTs, including those that are determined to be virtual assets. Uneven and often inadequate regulation and supervision allows regulatory arbitrage and can expose the U.S. financial system to NFT service providers operating abroad without adequate AML/CFT controls for the services being provided.

5. Mitigation Measures

The U.S. government's assessments take into consideration the effect of mitigating measures as part of the calculus to determine illicit finance risks. The below section explores how: (1) industry tools; (2) law enforcement authorities and public announcements; (3) the public nature of most blockchains; and (4) existing regulations and requirements for industry participants can each mitigate illicit finance risks associated with NFTs. The assessment finds that these measures may partially mitigate illicit finance risks but do not sufficiently address the identified vulnerabilities.

5.1 Industry Tools

Several industry participants are considering tools to mitigate risks of fraud and other illicit activities associated with NFTs. For example, there are online databases in which users and NFT platforms can search wallet addresses or website links to NFT projects for reports that the addresses or projects are linked to scams. While some of these databases require subscriptions or licenses, some of them are accessible for free. Free databases often rely on data provided by users and industry and are not vetted by law enforcement or other government authorities, but they can be a useful source of information to assess the potential for fraud or scams before

78 Stephanos Mitsios, "The New EU Markets in Crypto-Assets Regulation ("MiCAR")," EY, June 21, 2023, https://www.ey.com/en_gr/tax/tax-alerts/the-new-eu-market-in-crypto-assets-regulation; Outlier Ventures, "Written evidence submitted by Outlier Ventures," UK Parliament, April 18, 2023, https://committees.parliament.uk/writtenevidence/115627/html/#:~:text=The%20UK's%20light%2Dtouch%20regulatory,(%E2%80%9CFSMA%E2%80%9D)%20apply; "Guidance – Regulation of Virtual Asset Activities in ADGM," ADGM, December, 18, 2023, https://www.adgm.com/documents/legal-framework/guidance-and-policy/fsra/guidance-virtual-asset-activities-in-adgm-20231218.pdf; Facundo Sirena Isorni, Lucile Cesareo-Hostettler, Dominique Lecocq, "The Financial Technology Law Review: Cryptoassets, NFTs and DAOs: a Swiss Perspective," Lexology, May 11, 2023, https://www.lexology.com/library/detail.aspx?g=4975a78f-56b1-4ab0-91fb-2b078d6c209a.

79 "Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers," FATF, June 27, 2023, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html.

engaging in an NFT transaction. Similarly, NFT platforms can also utilize tools and databases to identify potential cases in which NFT content is used without the original creator's permission or NFT smart contracts that have been reported as related to scams. Other tools include the ability for NFT platforms to help detect and prevent fraudulent conduct and money laundering, including placing controls on the frequency of transactions by users to mitigate wash trading and other market manipulation or using blockchain analytics to identify potential users that may pose sanctions risks or to otherwise rate the risks of wallet addresses associated with users based on transaction history. These tools could be used by NFT platforms either to assist in meeting relevant regulatory obligations or voluntarily to protect the integrity of their platform and mitigate risks of their platform being used to launder illicit proceeds or from their users becoming victims to fraud or theft.

The administrators of NFT smart contracts can also implement measures to mitigate risks, including by conducting enhanced software reviews and quality checks, building in the ability to halt transactions using the smart contracts in instances of theft or other illicit activity, or using oracles to screen against digital asset wallet addresses appearing on sanctions lists and to prevent sanctioned addresses from using NFT smart contracts.

NFT platforms can also take other measures to improve their cybersecurity posture, including by enrolling in free Cybersecurity and Infrastructure Security Agency (CISA) Cyber Hygiene Scanning Services. CISA continuously scans for accessible services and vulnerability, while providing vulnerability alerts and suggested mitigations to enrolled firms.[80] NFT firms can also join the Financial Services Information and Analysis Center (FS-ISAC).[81] FS-ISAC is a non-profit, information-sharing forum established by financial services industry participants, shares among its members and trusted sources critical cyber intelligence, and builds awareness through a robust offering of alerts, indicators, member insights, threat assessments, and analysis.[82]

5.2 Applicability of Law Enforcement Authorities, Public Announcements

NFTs can be considered property in the United States for asset recovery purposes.[83] Therefore, law enforcement may subject NFTs to asset recovery laws and regulations like other property and have done so in at least one case related to NFT scams. While this does not necessarily prevent criminal misuse, it can afford law enforcement the ability to respond appropriately to crimes involving NFTs, as illustrated by the cases summarized in relevant sections of this assessment. This mitigation measure is further supported by the strength of the overall asset recovery regime in the United States. FBI has also issued public service announcements[84] and press releases to alert NFT users of potential threats and instruct users on how to defend against them. These publications also stress the importance that victims report fraudulent or suspicious activities to local FBI field office or via IC3.gov using the term "NFThack" to support law enforcement efforts. Reporting can play a critical role in initiating or supporting law enforcement investigations and resulting actions to hold accountable illicit actors in the NFT ecosystem.

80 "Cyber Hygiene Services," Cybersecurity & Infrastructure Security Agency, accessed August 13, 2024, https://www.cisa.gov/cyber-hygiene-services.

81 "FFIEC Releases Cybersecurity Assessment Observations, Recommends Participation in Financial Services Information Sharing and Analysis Center," Federal Financial Institutions Examination Council, November 3, 2014, https://www.ffiec.gov/press/pr110314.htm.

82 "What we do," FS-ISAC, accessed August 13, 2024, https://www.fsisac.com/.

83 See 18 USC 981(a)(1) (defining property subject to forfeiture as "any property, real or personal….").

84 "Criminals Pose as Non-Fungible Token (NFT) Developers to Target Internet Users with an Interest in NFT Acquisition," Federal Bureau of Investigation, August 4, 2023, https://www.ic3.gov/Media/Y2023/PSA230804, "FBI Las Vegas Federal Fact Friday: All About NFTs," FBI, July 22,2022, https://www.fbi.gov/contact-us/field-offices/lasvegas/news/press-releases/fbi-las-vegas-federal-fact-friday-all-about-nfts.

5.3 Public Blockchain Transparency

NFT transactions often occur on public blockchains, which means that in most cases any person with access to the internet can view the pseudonymous transaction data in the public ledger. Public ledgers can support investigations by competent authorities in tracing the movement of illicit proceeds. While the ledgers do not contain names or traditional account identifiers associated with any particular blockchain address, regulators and law enforcement can in some cases take viewable pseudonymous user and transaction information and pair it with other pieces of information to identify transaction participants.[85] However, there are some limitations to relying on public blockchain information and tracing to mitigate illicit finance risks, including the use of anonymity-enhancing technologies, off-chain activity, and cases in which there is no additional identifying information to attribute a pseudonymous blockchain address.

The uniqueness of each NFT token and, in some cases content, can support tracing individual NFTs that are the subject of theft, scams, money laundering, and other crimes or involved in money laundering. For famous, high-value NFTs in particular, ownership tracing is relatively easy since social media, NFT platforms, and other outlets publicizes high-profile and high-value sales. Victims of NFT theft have succeeded in retrieving their stolen NFTs through public campaigns, aided by the ability to provide the specific name, features, and token ID of stolen NFTs to competent authorities or successor owners of NFTs after the stolen NFT was resold.

5.4 Involvement of Covered Financial Institutions for NFT Transactions and Other Sources of Government Information

NFT platform users often rely on separate institutions including banks or money services businesses, such as those providing services in virtual assets, to interact with NFT platforms to facilitate the purchase of or to receive funds from the sales of NFTs. For example, users may connect their VASP account to an NFT platform to fund the purchase of an NFT. The extent to which financial institutions involved in NFT transactions effectively comply with AML/CFT and sanctions obligations could potentially mitigate illicit finance risks associated with NFTs and non-compliant NFT platforms. With effective BSA compliance measures in place at certain financial institutions, for example, competent authorities would likely be able to access customer or transaction information collected by the financial institution as part of AML program or recordkeeping requirements via legal process from the facilitating financial institution, if necessary, or the financial institution may report potentially suspicious activity involving their customer and the NFT platform. Additionally, if the transaction involved fiat currency, the facilitating financial institution may be required to file a Currency Transaction Report to FinCEN if the transaction exceeded $10,000.[86] Additionally, all NFT platforms conducting transactions involving U.S. persons are generally required to comply with sanctions regulations. Reliance on a third party for conducting sanctions screening would neither obviate sanctions compliance requirements nor preclude liability with respect to potential violations of sanctions regulations.

There, are, however, cases in which the facilitating financial institutions themselves may be non-compliant with AML/CFT or sanctions obligations. U.S.-based users may also use VASPs that are based in jurisdictions that lack or fail to effectively enforce AML/CFT requirements or comply with U.S. sanctions despite servicing U.S. persons for NFT-related transactions.

NFT platforms may have other regulatory obligations that can aid the collection of information that may support law enforcement investigations related to crimes involving NFTs. For example, transactions involving

85 For additional details on the benefits and limitations of mining data on the public blockchain, please see page 32 of the DeFi Illicit Finance Risk Assessment.

86 See 31 C.F.R. § 1010.311 (2024).

digital assets, including NFTs, are generally required to be reported on a tax return to the Internal Revenue Service (IRS).[87] Additionally, proposed tax regulations would require NFT platforms in the United States to collect certain transaction information, including the name and address of customers, for the sale of NFTs for the purposes of ensuring that taxpayers have relevant information and identifying potential tax evasion.[88] Such information may be made available by IRS to law enforcement agencies for the investigation and prosecution of non-tax criminal laws pursuant to court order.

6. Conclusion and Recommended Actions

The assessment identifies that NFTs and NFT platforms are to date rarely being used for proliferation financing or terrorist financing. However, this assessment finds that NFTs are highly susceptible to use in fraud and scams, many of which are traditional schemes that involve NFTs, and can be stolen from victims. Additionally, criminals use NFTs to launder proceeds from predicate crimes often in combination with other techniques or transactions meant to obfuscate the illicit source of funds. Criminals exploit vulnerabilities related to characteristics of NFTs, the assets or entitlements that they reference, and regulatory frameworks in the United States and abroad. In particular, cybersecurity vulnerabilities, challenges with trademark and copyright protection, and hype and fluctuating pricing of NFTs can enable criminals to perpetrate fraud and theft related to NFTs and NFT platforms. Moreover, some NFT firms and platforms lack appropriate controls to mitigate risks to market integrity, money laundering and terrorist financing, and sanctions evasion.

The assessment examined several mitigation measures that may partially address the identified threats and vulnerabilities, including: (1) industry tools; (2) law enforcement authorities and public announcements; (3) the public nature of most blockchains; and (4) existing regulations and requirements for industry participants, finding that these can partially mitigate illicit finance risks associated with NFTs.

Treasury has identified the following areas for further work to address outstanding risks.

- **Consider Application of Regulations to NFTs and Raise Awareness for Relevant Regulatory Obligations:** Relevant authorities should further consider regulations or guidance specific to NFTs and assess opportunities to provide additional clarity on existing obligations for applicable NFT platforms. For example, guidance, alerts, advisories, and other materials pertaining to digital assets could note how existing regulations and guidance apply to NFTs and NFT platforms. Private sector outreach could also raise awareness of relevant regulatory obligations and may help increase the number of compliant NFT platforms. If regulators identify any regulatory gaps in their framework applicable to NFTs, they should identify ways to address those gaps. However, weighed against other sectors, including other elements of the digital asset ecosystem, that pose greater money laundering and terrorist financing risks, addressing any gaps applicable to NFTs should not be prioritized over existing regulatory priorities.
- **Continue to Enforce Existing Applicable Laws and Regulations:** U.S. regulatory agencies should continue to supervise and, as appropriate, take enforcement actions for actors in the NFT sector that fail to comply with applicable obligations, including BSA and sanctions obligations.

87 "Digital Assets," Internal Revenue Service, February 28, 2024, https://www.irs.gov/businesses/small-businesses-self-employed/digital-assets.

88 "Gross Proceeds and Basis Reporting by Brokers and Determination of Amount Realized and Basis for Digital Asset Transactions," Internal Revenue Service, August 29, 2023, https://www.federalregister.gov/documents/2023/08/29/2023-17565/gross-proceeds-and-basis-reporting-by-brokers-and-determination-of-amount-realized-and-basis-for.

- **Continue Private Sector Engagement to Support Understanding of Developments in NFT Ecosystem:** The rapidly evolving nature of both NFT use cases and NFT platforms requires further research and engagement with the private sector. The U.S. government should continue to monitor changes in the NFT ecosystem in order to understand how these changes may impact the AML/CFT obligations of platforms and illicit finance risks within the NFT space. In addition, applicable NFT firms could benefit from enrollment in a CISA Cyber Hygiene Scanning Service and participation in FS-ISAC.
- **Encourage Industry to Address Scams and Fraud:** The U.S. government should engage with developers and other industry stakeholders to promote innovation that seeks to mitigate the illicit finance risks of NFTs and NFT platforms, especially risks relating to scams and fraud.
- **Educate Consumers:** The U.S. government and industry stakeholders should consider providing educational materials to improve consumer understanding about rights that may or may not convey with NFTs and reduce consumer confusion.
- **Engage with Foreign Partners:** The U.S. government should engage with foreign partners to encourage risk assessments and development of policy approaches to addressing illicit finance risks of NFTs and NFT platforms.

7. Methodology

This report incorporates published and unpublished research and the analysis, insights, and observations of managers and staff from U.S. government agencies, which also reviewed this report. In drafting this assessment, Treasury's Office of Terrorist Financing and Financial Crimes (TFFC) consulted with staff from the following U.S. government agencies, who also reviewed this report:

- **Department of Homeland Security**
  - Homeland Security Investigations
  - U.S. Secret Service
- **Department of Justice**
  - Criminal Division
    - Money Laundering and Asset Recovery Section
    - National Cryptocurrency Enforcement Team
  - Drug Enforcement Administration
  - FBI
    - Virtual Assets Unit
- **Department of State**
  - Bureau of Economics and Business Affairs
- **Department of the Treasury**
  - Domestic Finance
  - Internal Revenue Service Criminal Investigations
  - International Affairs
  - Office of Terrorism and Financial Intelligence
    - FinCEN
    - OFAC
    - Office of Intelligence and Analysis
- **Staff of the federal functional regulators**[89]

89 This includes staff of the Commodity Futures Trading Commission (CFTC), the Office of the Comptroller of the Currency (OCC), and the Securities and Exchange Commission (SEC).

The authors of this report also conduct several meetings with U.S. government operational agencies and used open-source reporting from Treasury's risk assessments, open-source reporting from the DOJ, and available court documentation.[90] The risk assessment was also informed by consultations with several U.S. government Departments and Agencies and the over 75 responses to Treasury's Request for Comment, which was issued in conjunction with the publication of the "Action Plan to Mitigate Illicit Finance Risks of Digital Assets."

The terminology and methodology of this risk assessment are based in part on the guidance of the FATF, the international standard-setting body for AML/CFT safeguards. The following concepts are used in this risk assessment:

- **Threats**: For purposes of this assessment, threats are the predicate crimes that are associated with money laundering as well as individuals or entities, or activity undertaken by those individuals and entities, with the potential to cause a defined harm. The environment in which predicate offenses are committed and the proceeds of crime are generated is relevant to understanding why, in some cases, specific crimes are associated with specific money laundering methods.
- **Vulnerabilities**: Vulnerabilities are what facilitate or create the opportunity for misuse of NFTs to transfer or move funds to launder the proceeds of crime, finance terrorism, or acquire materiel or support revenue generation for weapons of mass destruction programs. They may relate to a specific financial sector or product or a weakness in law, regulation, supervision, or enforcement.
- **Consequences**: Consequences include harms or costs inflicted upon U.S. citizens and the effect on the U.S. economy, which provide further context on the nature of the threats.
- **Risk**: Risk is a function of threat, vulnerability, and consequence. It represents an overall assessment, taking into consideration the effect of mitigating measures including regulation, supervision, and enforcement.

90 The charges contained in an indictment are merely allegations. All defendants are presumed innocent unless, and until, proven guilty beyond a reasonable doubt in a court of law.


THE DEPARTMENT OF THE TREASURY
1789