J5 JOINT CHIEFS OF GLOBAL TAX ENFORCEMENT

J5 Releases NFT Red Flags to Warn Public of Risks

April 28, 2022

WASHINGTON – The Joint Chiefs of Global Tax Enforcement (J5) announced the release of an intelligence bulletin today, warning banks, law enforcement personnel and private citizens of some of the dangers when dealing with Non-fungible Tokens (NFTs).

The document, called the “J5 NFT Marketplace Red Flag Indicators,” is the first of its kind from the J5. It lists items that should draw concern when one is dealing with NFTs or planning to purchase one. The document is not meant to be an all-inclusive list of risks associated with NFTs, but rather a list of best practices from the five countries in the J5 from their dealings with NFTs in various investigations. While the majority of cryptocurrency owners and those purchasing NFTs are doing so for righteous reasons, criminals look for any way to exploit new technologies. Cryptocurrencies and NFTs are not immune.

“This space is changing so fast and technologies and products have the ability to become the ‘next big thing’ without any due diligence or regulation on the part of the creator of the product,” said Special Agent Oleg Pobereyko, J5 Crypto Group Lead. “We tried to put together a product that would help keep people safe while law enforcement catches up to these particular concerns.”

The purpose of this document is to provide insight to banks, law enforcement partners and private industry regarding potential red flags in NFT Marketplaces. The J5 seeks to continuously improve fraud detection measures in place to detect and prevent criminal activity. NFTs can be anything digital including drawings, music or anything that can be seen as art. They have been described as an evolution of fine art collecting, only digital.

The J5 recognizes that data available to NFT Marketplaces can provide additional and valuable perspectives in combatting fraud. A list of possible account or transaction attributes are included in the document that may provide these insights. It is likely that any single indicator in isolation will not be a definitive indication of fraud, however a compound set of risk indications, after following a “Business as Usual” process, may provide insights into potential fraud:

“I hope this is the first of several of these intelligence bulletins the J5 puts out,” said Jim Lee, Chief, IRS Criminal Investigation. “We are doing incredibly innovative things in the J5 and the lessons we are learning are cutting edge. Sharing that information with the public and private sectors can only help to stop various types of fraud before they become the next case on our investigative inventory.”

“Cryptocurrency is growing in popularity in Australia, with many choosing to invest as part of their portfolio,” said ATO Deputy Commissioner and J5 Chief Will Day. “This paper provides a suite of indicators that financial institutions can reference to help them identify illicit financial activity concerning NFTs. It's intended to be the first of many that can be used by financial institutions to assist in the fight against tax crime and money laundering involving virtual assets. This report is a unique and progressive initiative and the J5 looks forward to working closer with the virtual assets industry to meet the rapidly evolving and highly complex environment which we share."

Next month, J5 members will come together in London, England for a variety of meetings – one of which is called the J5 Challenge. The event brings together experts from each country with the mission of optimizing data from a variety of open and investigative sources available to each country, including offshore account information. Using various analytical tools, members of each country will be put into teams and tasked with generating leads and finding tax offenders using cryptocurrency based on the new data available to them through The Challenge. This will be the fourth iteration of the Challenge. Working within existing treaties, real data sets from each country were brought to the challenge to make connections where current individual efforts would take years to make those same connections.

The J5 leads the fight against international tax crime and money laundering, including cryptocurrency threats and those who undertake, enable or facilitate global tax evasion. They work together to gather information, share intelligence and conduct coordinated operations against transnational financial crimes. The J5 includes the Australian Taxation Office, the Canadian Revenue Agency, the Dutch Fiscal Information and Investigation Service, Her Majesty's Revenue and Customs from the U.K. and IRS-CI from the U.S.

For more information about the J5, please visit www.irs.gov/j5.

J5 NFT Marketplace
RED FLAG INDICATORS

Introduction

The J5 was formed in 2018 after a call to arms from the OECD Taskforce on Tax Crime and has been working together to gather information, share intelligence and conduct coordinated operations, making significant progress in each country's fight against transnational tax crime. The J5 includes the Australian Taxation Office (ATO), the Canada Revenue Agency (CRA), the Dutch Fiscal Information and Investigation Service (FIOD), Her Majesty's Revenue and Customs (HMRC) from the UK and the Internal Revenue Service Criminal Investigation Division (IRS-CI) from the US.

The purpose of this document is to provide insight to banks, law enforcement partners and private industry regarding potential red flags in NFT Marketplaces. The J5 seeks to continuously improve fraud detection measures in place to detect and prevent criminal activity. This document is not meant to be all-inclusive, but rather a collection of insights and best practices gained from investigations

Fraud Insight from the Sector

The J5 recognizes that data available to NFT Marketplaces can provide additional and valuable perspectives in combatting fraud. A list of possible account/transaction attributes follows that may provide these insights. Some of this may be possible to derive from transactional activity alone, and some may be part of KYC or normal client relationship data held. It is likely that any single indicator in isolation will not be a definitive indication of fraud, however a compound set of risk indications, after following a "Business as Usual" process, may provide insights into potential fraud:

Strong Indicators:

- Newly minted or secondary market transactions of > USD 100,000 with no observable community.

- A network of sending and receiving parties to the same transaction or group of transactions.

- Newly minted NFTs held by subjects being sold at high price points immediately which is not in line with others in the collection (potentially hiding the true reason for purchase)

- NFTs being sold for large sums and reacquired from the same party or a third party for smaller amounts would be a strong indicator.

- The turnover low value NFTs quickly. For example, on Top Shots with the NBA you see a lot of low value (i.e. sub 10K) NFTs being bought in the same day with owners only holding their position for minutes. This could be a way to wash funds – so owning for very short periods.

- Clearly overpriced/underpriced NFT that is traded frequently in short time windows.

- Wash trading – artificially increasing sale value with each sale, between linked accounts.

- Incorrect Mint Address - contract address doesn't match address provided on project website.

- Requiring seed phrase from Ethereum wallet in addition to the MetaMask wallet address for a transaction to be executed.

- Phishing scams: fake offers on NFTs, sent via email.

- Fake token give-aways/airdrops.

- Social media impersonation – unverified accounts that also have no active followership and engagement.

- Similar NFT collections - copy to exploit for fraud

- Significant number of sales in a collection purchased from a mixer

- NFT collection from high-risk area

- Price - If there is a huge price gap, normally lower, between the site and a legitimate marketplace then there is reason to believe it is a scam.

Moderate Indicators:

- Smaller amounts broken down into Multiple transactions such as > USD 10,000 x 5, for a period, with no observable community. *Caution should also be exercised when looking at this indicator in isolation as this might also be caused by software testing.*

- Re-used code within the NFT. *It is also important to note that it is common to share code in the software development community, so this indicator alone is not definitive*.

- Minting an NFT, buying it at an inflated price and selling for a considerable loss. For instance, a buyer acquires an NFT for $1M and sells it for $750K in a very short time. *This might also be due to general volatility of the markets, so extra considerations would need to be made before coming to a conclusion.*

- No Thumbnail on marketplace profile. *Note, like the other indicators above, this indicator in isolation is not definitive.*

- No checkmark for verification on market profile (*Note, like the other indicators above, this indicator in isolation is not definitive*):

    a. Verified accounts with a blue checkmark (OpenSea). However, legitimate accounts can be hacked by illicit actors who then use the accounts for their laundering/scams.

- Non-existent contract address (Ethereum) for traceability on the project (*Note: some legitimate projects have also exhibited this*).
    a. No clarity on when and where the NFT was minted.

- Properties and project description fields of the NFT are empty or not clearly stated (*Note: some legitimate projects have also exhibited this*).

- Significant number of sales in a collection purchased from same or clustered wallets

J5