Financial crime in the metaverse is real – how can we fight back?

October 2022

Fighting financial crime in the metaverse requires a multi-level approach

The metaverse merges social life, leisure, technical and crypto innovations to create new and exciting ways for people to interact virtually. Like the real world, however, the virtual one is not immune to criminal activity. Due to their increasing popularity, value and use cases, crypto-assets have become the target of criminal efforts. Awareness of typical threats, exchange of best practices and cooperation on national and international levels are key to successfully prevent and fight financial crime in the metaverse.

Summary of key points:

- Due to the increasing popularity and value of crypto-assets, financial crime has become a threat in the innovative digital market of the web3.0 metaverse.
- Users and companies need to familiarise themselves with typical criminal activities in the metaverse, such as phishing and fraud scams, code exploits, wash trading, money laundering and terrorist financing to protect themselves and others.
- Financial crime in the metaverse is a growing challenge for law enforcement due to its cross-border dimension and requires a common and effective criminal law approach to protect market players without stifling innovation.

What is the web3.0 metaverse?

Web3.0 Metaverses combine immersive experiences with entertainment in a three-dimensional virtual world. People interact with others using headsets and their online avatars that enable them to move, speak and act freely. In the metaverse, players can explore an alternative reality with shops, offices and entertainment facilities, where the laws of physics no longer apply – only the rules and limits one imagines. They can inhabit their own spaces, own and even create virtual property, such as art or buildings, and sell that property to other metaverse users.

Web3.0 metaverses are typically gamified and decentralised, hence the names of the popular Ethereum-based virtual worlds ‘The Sandbox’ and ‘Decentraland’. A decentralised metaverse is not owned by a single entity, like a company, but by the metaverse community. Users can control their experience almost entirely, including the way the metaverse is built and operates. They can own, buy and trade goods, land, services and applications by utilising crypto-assets.

Crypto-assets in the metaverse

Living, working and playing in an alternate reality requires funds, and in the metaverse, that means crypto-assets. Crypto-assets are digital representations of value or rights which may be transferred and stored electronically, using distributed ledger technology – such as blockchain – or similar technology (see Art. 3 para. 1 no. 2 of the Proposal for a Regulation on Markets in Crypto-assets, COM(2020) 593 final).

To acquire, access and trade crypto-assets, a person needs a so-called digital wallet. However, a digital wallet never contains the actual assets, only their owner's cryptographic keys to access them: the public key – comparable to an IBAN – and the private key – the PIN code to the wallet. The crypto-assets as such exist only on the blockchain with which the wallet interacts.

> The value and popularity of crypto-assets have increased significantly, which makes them an attractive target for financial crime.

Due to new investments in metaverse projects, celebrity involvement and expanding use cases, the value and popularity of crypto-assets have increased significantly. Among crypto-assets, Non-fungible Tokens (NFTs) have particularly gained popularity in the fields of art, music, gaming, sports, entertainment and even politics. NFTs are unique digital certificates that can authenticate digital artworks and prove ownership within metaverses. Also, they can be collected, sold and traded on various online marketplaces. Some NFTs are valued at millions of dollars, which makes them a target for scams, wash trading, and money laundering: from July 2021 to July 2022, over US $100 million in NFTs was stolen according to the blockchain analytics company Elliptic.

Types of financial crime in the metaverse

Not surprisingly, financial crime has entered the metaverse as well. The consequences are severe, not only for the victims but also in the context of slowing progress and technical innovation. As stated by the EU legislator, fraud does not only enrich criminal groups, but also limits the developments of the digital market and makes citizens more reluctant to make online purchases (*cf.* recital 7 of the Directive (EU) 2019/713).

To raise awareness of how criminals can exploit the new opportunities created by the metaverse, typical forms of financial crime are highlighted below.

a) Phishing and fraud scams

One of the most common threats is the various types of phishing and fraud scams that occur. According to a report by Elliptic published in August 2022, US $14 billion worth of crypto-assets were reported stolen due to scams in 2021 alone.

Phishing scams often involve malicious fake sites designed to compromise victims' crypto assets. Those sites can imitate the login panel of a legitimate wallet provider, an NFT market or a well-known metaverse like Decentraland, so that the users click on the phishing link instead of the official domain. Users think that they are accessing or connecting via their wallets, while in reality they provide the scammers with the private data to their wallets and find their assets stolen by the scammers as a result.

One of the most successful methods used by cyber criminals is social engineering. Because exploiting individuals' psychological vulnerabilities is so effective in general, this has already become a major challenge in the metaverse as well. There are many ways scammers can gain people's trust. They can pretend to represent legitimate metaverse projects, e.g. by gaining control of well-known social media accounts, by impersonating trusted institutions or avatars in the metaverse, and by tricking people of the community to click on a phishing link or to send funds to the scammers' wallet. Scammers can also pose as support staff for metaverses or wallet services and trick users into sharing private keys or direct them to a fake site by pretending that they want to help them with some technical issue.

> Scammers try to gain users' trust by pretending to represent legitimate metaverse projects and tricking them in to clicking on a phishing link or sending funds to the scammers' wallet.

A major fraud risk for crypto investors is what is known as a rug pull, which refers to all of the ways developers of a cryptocurrency project abandon it unexpectedly, taking users' funds with them. When establishing a metaverse project, developers will first detail their plans in a roadmap including online game development or charity fundraising and then start campaigns to raise funds to take the project to the next stage. Scammers, however, capitalise on the initial excitement of a new project. They try to get investors to buy in a fake or low quality metaverse project and then "pull the rug" – pull as much value out of the project as possible, leaving investors with a worthless project or simply disappear with the funds.

b) Code exploits

Another way to steal people's crypto-assets is by using malware which targets digital wallets. Cyber extortion and ransomware are notorious and very lucrative cybercrime threats, and they pose a serious risk in the metaverse as well, considering how a metaverse is created. Many metaverses exist as a complex web of smart contracts, i.e. self-executing codes on a blockchain, governing the interactions between assets and services in the metaverse. Bad actors have already been exploiting vulnerabilities in the underlying software or smart contracts used, including in metaverse-related projects.

c) Wash trading

A wash trade is a form of market manipulation where investors sell their own assets to themselves or a co-conspirator to create misleading, artificial activity on a market. This can have several nefarious goals: a wash trader selling assets for an undervalued amount might attempt to report a loss for tax purposes. If wash traders overvalue their assets, they could try to drive up the perceived value of their tokens so they can sell them to others for higher prices.

The simplest form of wash trading is one user rapidly reselling a token at a much higher or lower price than what it was purchased for. The wash trader can also use multiple wallets that either belong to the same user or to close associates: A sells an NFT to B, then B re-sells the NFT back to A for a very different price.

d) Money laundering, sanctions evasion and terrorist financing

From the perspective of the perpetrator, money laundering serves to conceal the illegal origin of a means of payment. The metaverse can be used as a channel to launder illicit funds, whether they stem from real-world or crypto-based crime. Funds can be exchanged for metaverse-based assets such as land, NFTs, or metaverse-related crypto assets. Perpetrators can also try to use the metaverse to raise funds for sanctioned actors, including those linked to terrorism, via metaverse-related assets.

> The metaverse can be used as a channel to launder illicit funds or to raise funds for sanctioned actors, including those linked to terrorism.

On the EU level, the 5th Anti-Money Laundering (AML) Directive (EU) 2018/843 explicitly considered virtual currencies and extended AML obligations to providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers. Several wallet providers and cryptocurrency exchanges, like Coinbase or Binance, have already implemented Know-your-customer (KYC) checks. However, there are still many cryptocurrency exchanges that enable crypto transactions without any such controls or verifications. Likewise, KYC checks are not yet required to purchase goods on several metaverse or secondary marketplaces, which facilitates attempts to launder money or provide funds to sanctioned actors.

On the other hand, the fact that every single transaction on a blockchain is transparent might be a powerful deterrent, especially when it comes to criminal exploits of NFTs. An NFT's page on a marketplace can provide a complete history of transfers, bids, listings etc., and links to related transactions and buyers' or sellers' wallets can provide even further insights, which makes NFTs one of the most transparent assets on a blockchain. As such, they are easily traceable by investigators and very unattractive for illicit actors.

How users and institutions can fight back

As these examples indicate, preventing and fighting financial crime in the metaverse is a complex endeavour that requires multiple stakeholders to work together. End-users need to be aware that participating in any new technology makes them a potential target of criminal actors. To protect against phishing attacks and fraud scams, people should remind themselves to think critically and not let their "fear of missing out" lead to impulsive decisions. Companies working in the metaverse should collaborate with their security and risk teams early on to identify possible vulnerabilities, train their developers about these risks, and test apps thoroughly before they go live. To protect against code exploits, users and companies should engage with metaverse projects whose smart contract codes have been developed and audited by a technically strong and reputable team. To assess the risk of wash trading, it is important to review the trading volumes against historical trends. For example, where trade history is limited, price drivers regarding land or wearables must be considered, such as proximity to key locations and the provenance of an NFT collection creator.

Additionally, financial crime in the metaverse does not occur outside the system of legal protection safeguarding users. Even though tracing the international networks of faceless criminals is a challenge for law enforcement, there have been significant efforts to develop an effective criminal law approach to prevent and fight crime related to crypto-assets. The EU has been very active in issuing directives to align the respective national legal frameworks, e.g. the 5th AML Directive (EU) 2018/843 and the Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment. The Proposal for a Regulation on Markets in Crypto-assets (MiCA) defines the regulatory treatment of crypto-assets and includes measures against market manipulation, money laundering, terrorist financing and other criminal activities.

In Austria for example, financial crime in relation to crypto-assets can fall under various domestic criminal law offences, e.g. illegal access to a computer system ("hacking", Sec. 118a Criminal Code, "**CC**"), data corruption (Sec. 126a CC), disruption of the functionality of a computer system (Sec. 126b CC), spying-out data of a non-cash means of payment ("phishing", Sec. 241h CC), extortion (Sec. 144 CC), fraud (Sec. 146 *et seqq* CC), money laundering (Sec. 165 CC) and terrorist financing (Sec. 278d CC). As each country has its own laws in this evolving industry, seeking to understand the local laws for crypto-assets can help users and companies to be aware of potential threats and limitations while at the same time taking advantage of all the positive opportunities the metaverse has to offer.

Understanding the local laws for crypto-assets can help users and companies to be aware of potential threats and limitations while at the same time taking advantage of all the positive opportunities the metaverse has to offer.

The metaverse allows its users, including criminals, to interact virtually. In addition to companies raising awareness and individuals being alert about potential foul play, policy and law makers are key in protecting companies and individuals from criminal activities in the metaverse. They bear the responsibility to strike the balance between, on the one hand, implementing effective regulations and, on the other, enabling and promoting technical innovation – a process that requires ongoing exchange of best practices and cooperation on national and international levels.

About Wolf Theiss

Wolf Theiss is one of the leading European law firms in Central, Eastern and South-Eastern Europe with a focus on international business law. With 340 lawyers in 13 countries, over 80% of the firm's work involves cross-border representation of international clients. Combining expertise in law and business, Wolf Theiss develops innovative solutions that integrate legal, financial and business know-how.

For more information about our services, please contact:

Angelika Zotter
Associate

E angelika.zotter@wolftheiss.com
T +43 1 51510 5472