We need to anticipate and address potential fraud in the metaverse

September 8 2022, by Nadia Smaili and Audrey de Rancourt-Raymond

Credit: AI-generated image (disclaimer)

The metaverse is a virtual online world that people can access in a variety of ways, including through virtual and augmented reality. It offers people an interactive social experience where users are represented by avatars. Users can teleport through different virtual social worlds, participate in events and make transactions using

cryptocurrencies.

By 2026, it is predicted that 25% of people will spend at least one hour a day in the metaverse. There, they'll be able to participate in activities such as working and shopping, and 30% of firms will have their products and services ready for the metaverse.

The metaverse—which includes blockchains and cryptocurrencies—is still in its early stages. As its possibilities expand, it's important to consider the potential threats and dangers as the metaverse introduces risks related to legislation, property, control, fraud, privacy threats, ethics and security.

As researchers interested in forensic accounting and digital fraud, we have attempted to identify the risks that are unique to the metaverse.

Opportunity or threat?

The metaverse appears to be a foray into developing new models of conducting business online. And as such, can we anticipate the related risks? Are current laws applicable to the metaverse? How are we protected from fraud in the metaverse?

While the metaverse offers new opportunities for firms and customers, as a nascent technology, it comes with multiple risks.

Breaches in ethics are possible. For example, do firms consider whether their code of ethics has been updated to account for expansion into the metaverse? How do customers and employees behave in the metaverse? Is sensitive information protected?

Legal issues will relate to intellectual property rights, the regulation of virtual assets, privacy and gambling. Firms considering using the

metaverse should anticipate intellectual property rights, in particular those related to terms of service agreements and end-user license agreements.

Metaverse fraud risks

The metaverse can bring many fraud risks, such as market manipulation, cyber breaches and attacks, privacy breaches, money laundering, corporate espionage and identity theft.

Unlike traditional social media platforms, users have no guarantee that the data they share is only shared with those they choose to share it with in the metaverse. That means user identities can be tracked and revealed

As one researcher explains: "We cannot just turn off who can follow our avatars in the metaverse as we can do in the traditional social media."

Personal information, such as biometric data, can be collected through the metaverse and in turn used for marketing purposes. Organizations using the metaverse need to ensure data is anonymized and users cannot be identifiable.

The rapid development of the metaverse has also brought risks related to cryptocurrencies, which are already subjected to very little official regulation. Scams could potentially flourish in the metaverse—and at worse, become normalized as a metaverse experience.

Preventing fraud

Risks in the metaverse can be mitigated by corporations and governments implementing controls that ensure users and administrators are protected. These are steps that can be taken to deter, prevent and

detect fraud in the metaverse.

In our research on identifying potential fraud in the metaverse, we identified two sets of actions: macro, which take place at the government level, and micro, which affect corporations.

At the government level:

- Specific regulation is needed for the metaverse, possibly in the form of a new Metaverse Act that encompasses metaverse transactions and actions;
- Increased oversight by government bodies, such as financial authorities;
- Establishment of an international and global authority to oversee the metaverse;
- Co-operation with businesses to share information that will reduce risks and prevent malicious use and unethical behavior and misinformation in the metaverse;
- Regulatory bodies should require or encourage organizations to disclose how they mitigate metaverse risks, what resources they have, and how they protect users from identity theft, misinformation, cyber threats and privacy breaches.

At the level of individual corporations or organizations active in the metaverse, here are some steps that can be taken:

- Adopt a comprehensive internal approach within different departments (for example auditing, marketing and finance departments) to identify weaknesses when processes are implemented in the metaverse;
- Implement measures that regulate avatar behavior on different platforms to ensure users conform to community standards;
- Employment of artificial intelligence to combat fraud and scams;

- Update codes of ethics and whistleblowing programs to protect whistleblowers and facilitate whistleblowing channels;
- Ensure that an adequate program is in place to mitigate and respond to metaverse threats.

Boards of directors, governance bodies and management should be trained and able to co-ordinate efforts to combat the emergence and the expansion of crime in the metaverse. Training and education are the first steps in establishing an efficient metaverse anti-fraud program.

Provided by The Conversation