breakroom sinespace

WHITE PAPER

MANAGING RISK
In the Metaverse

WRITTEN BY:

Frank Morisano,
Treliant, LLC

IN PARTNERSHIP WITH

Breakroom

About Breakroom

Breakroom is the next evolution in digital collaboration and engagement. Our immersive 3D environment creates an engaging digital experience that empowers connection, collaboration, and communication. Our leading-edge Metaverse platform is full of robust functionality that makes it easy for you to instantly create and customize your own branded virtual world, suitable for all types of audience engagement. From digital workspaces, conferences, and virtual classrooms to film festivals, book launches, and social events, Breakroom allows you to do it all.

CREATE A WORLD PEOPLE WANT TO BE A PART OF!

Page of Contents

About the Author

Frank is an internationally recognized executive with 30 years of proven accomplishments: growing businesses, steering profitable growth, leading the acquisition, divestment and restructuring of companies, developing companies' risk and financial crime capabilities, and implementing environmental, social, and governance standards, frameworks, and disclosure reporting software to follow global regulatory requirements.

Frank was recently the Chief Risk Officer at Industrial and Commercial Bank of China with responsibility for the Americas risk profile. Prior executive management roles include the leadership of revenue-generating businesses at PwC, GMAC, JPMorgan Chase, and Bank of America. He also serves on private and public boards as a non-executive and independent director.

Frank received his credit training at the Chase Manhattan Bank, holds an MSc in Information Systems, and a BBA in Statistics. He is a frequent speaker on emerging topics: artificial intelligence, data analytics, digital assets, sustainable finance, ESG, and information security.

Frank Morisano
Senior Managing Director
Treliant, LLC

Introduction

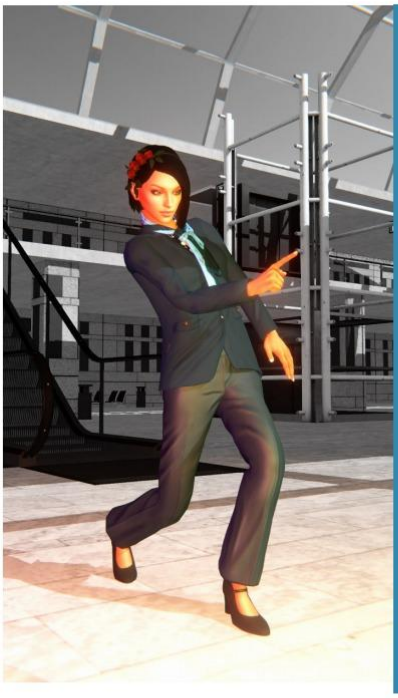
With so much buzz about the Metaverse, it's easy to see why more and more companies, educational institutions, and individuals have begun to conduct business in the virtual world. The question to individuals, company management, and Boards is, are they thinking about the risks and dangers they will encounter and need to overcome in these virtual worlds?

The Metaverse comprises multiple platforms that allow individuals to engage and accomplish their digital objectives through virtual and augmented reality. The virtual world permits users to communicate with each other using 3D avatars and exchange intelligence via human-computer interaction ("HCI"). Companies across a wide range of industry sectors are capitalizing on the commercial potential of the metaverse.

The complex structure of these virtual worlds requires companies to navigate and overcome a patchwork of existing and emerging regulations, laws, and risks to operating successfully. Recent estimates suggest the global metaverse market will be over $900 billion by 2030 compared to about $20 billion in 2021.

Race to the Metaverse

Beyond the games, marketing posters, business centers, and company headquarters on virtual land, the Metaverse is about commerce. Globally, companies are racing to create immersive 3D virtual experiences for consumers. For many companies, the investment comes from the marketing budget rather than the balance sheet.



Once in the metaverse, a company and consumer can create, buy and sell anywhere, seamlessly and without technological or geographical borders. From a marketing perspective, any financial gains or brand reward points a client earns in a virtual world can be used to buy real-world goods in the outside world.

Technological Factors

Two technological factors make up the Metaverse. First, an online 3D world connected to your real world through augmented or virtual reality that enables access to alternate or simulated reality. Gaming platforms are the perfect example, but they do not all work together as the Metaverse is decentralized.

Second is digital ownership, where the Metaverse assets are tied to cryptocurrencies permitting spending and the ability to earn by providing goods and services inside the Metaverse. Blockchain provides the foundation technology to buy, sell and prove ownership. Nonfungible tokens ("NFT"), also based on blockchain, represent real estate, art, song, and other objects of value. With cryptocurrency, you can also buy real estate the same as you purchase an NFT. It represents your ownership by one-of-a-kind code on a blockchain. In the Metaverse, one's identity is defined by the metadata on their blockchain. Trust within the ecosystem is built through blockchain activity independently verified by a decentralized network.

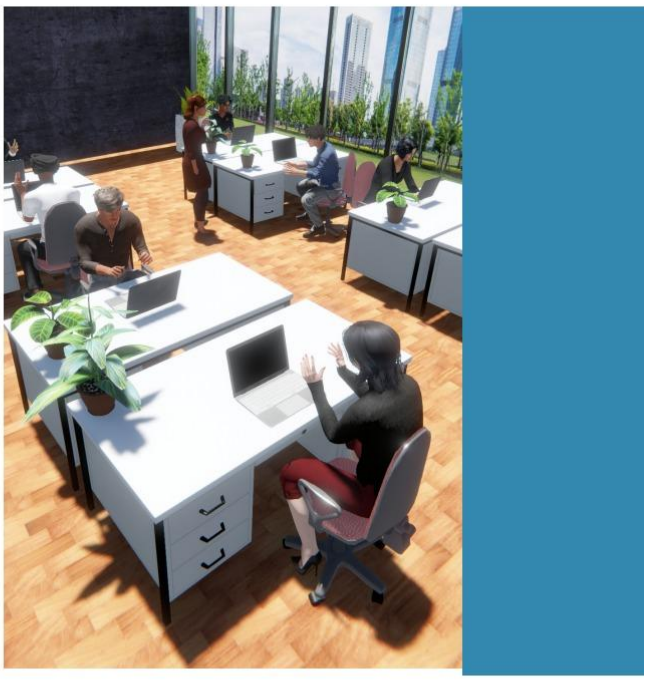
Corporate Governance

No new frontier is without risk and dangers, which is certainly the case for these virtual worlds. Businesses and clients need to understand that any current example of the Metaverse is neither a single destination nor a fully realized digital environment. The Metaverse at present is a collection of vastly different emerging digital platforms, some public, and others private, each built and advertised for their own purposes. As such, the metaverse contains familiar and new risks to all participating.

The need for corporate governance in these virtual worlds is clear - as technology increases, the ability of any one entity to govern decreases. The Metaverse infrastructure is being created and expanded by technology companies with minimal government oversight or regulations. The most significant risk to these virtual worlds is the lack of a secure environment at the foundation, meaning the decentralized blockchain platform that makes it more challenging to regulate. Blockchain's decentralized and unregulated nature permits the theft of virtual assets or money laundering to occur until governments openly address the legal and risk considerations easily.

As individuals and companies build their Metaverse infrastructure, they must proactively look at the potential risks and liabilities, not just the positives created by the virtual worlds. Additionally, they will need to enhance all three lines of defense (business, risk management, and internal audit) with the skills required to verify transactions and financial market regulations like anti-money laundering ("AML") and know-your-customer ("KYC").

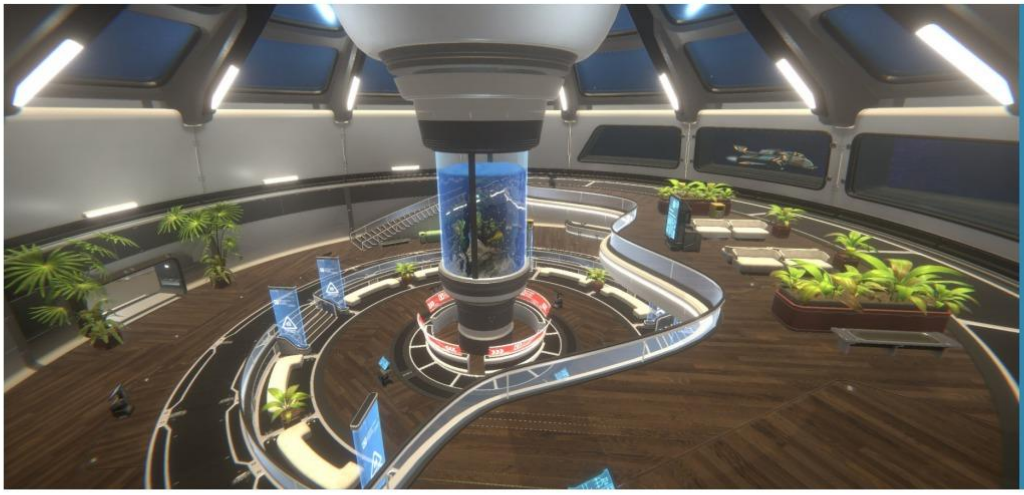
Key challenges and material risks arising from the Metaverse include cyber security, identity and data privacy, harassment and assault, financial crime, and fraud.



Implications for Cyber Risk

Virtual worlds and digital platforms have significant implications for cyber risk. As fast as the Metaverse is developing, threat actors are testing unique ways to benefit from potentially insecure network protocols or holes in its aging technology infrastructures. Within these virtual worlds, individuals and companies use immersive digital technologies, permitting malicious actors more entry points for cyberattacks and data breaches. Attacks have been known to range from standard account takeover and phishing attacks to more complex attacks, such as hosting fake services to hijacking digital data. It is worth noting that attacks can come from other individuals, the company sponsoring the virtual world, not just external actors.

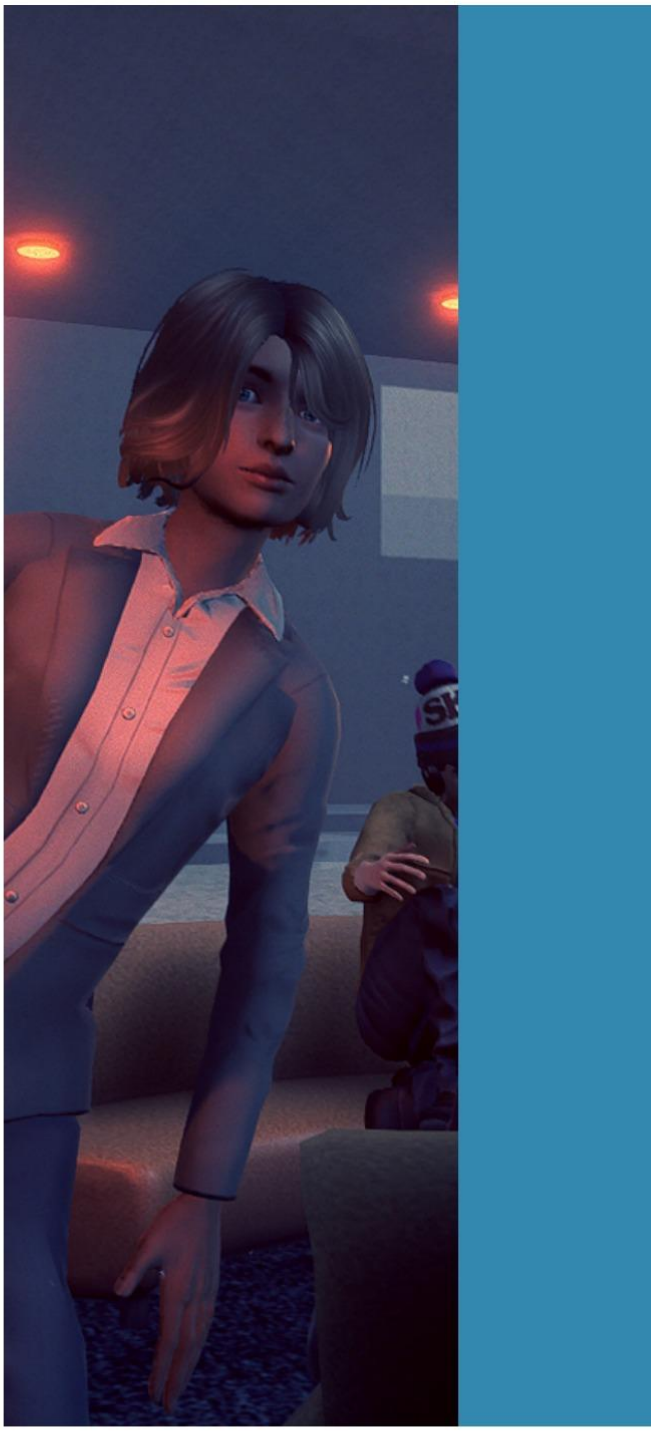
Moreover, 3D experiences could make some cyberattacks deeply traumatic to individuals. Virtual platforms also increase online reliance, which makes addressing the data privacy question critical for all participants. Digital identity in a virtual world is much easier to create than physical identification cards issued by governments. The data collected about an individual through a connected device includes biometric data, age, health information, data revealing racial and ethnic origin, voice recordings, and other personal data requiring consent. This data is a goldmine for technology companies, marketers, and hackers.



Given the nature of the virtual worlds and the extra-territorial reach, companies must ensure they comply with jurisdictional and age regulations.

Data in these virtual worlds may reside in multiple versions, on multiple cloud platforms, and in different jurisdictions. Data protection and privacy laws, such as the European Union's General Data Protection Regulation ("GDPR") or the California Consumer Privacy Act ("CCPA"), are designed to be technologically neutral; however, the virtual platforms create complex challenges to identity and data privacy due to the quantity and breadth of personal data that could be generated through user engagement. Hence, personal and sensitive information can be through a multitude of virtual worlds.

Individuals must be vigilant in protecting their personal information and digital identities and ensuring that their digital footprints are masked in real time to prevent identity fraud. Not only is data privacy and identity theft an unsolved and growing metaverse issue, but the hardware used by individuals has been proven to be full of security vulnerabilities, such as simple privacy protection policies and the lack of multifactor authentication. Never depend on the owners of the virtual world to protect your data or assist you with resolving an incident.



Bullying and Harassment

In a virtual world similar to the workplace, unwanted interactions such as harassment can occur. Harassment may be focused on verbal bullying, blatant physical or sexual abuse, grouping, and unwanted, unwarranted attention. Companies and individuals should not underestimate the potential impact of virtual world harassment. Researchers suggest that because the human experience in these virtual worlds is as real as our experience in the real world, the pain and suffering may seem as real and as intense.

This bad behavior in virtual worlds is not new, and Meta researchers reported recently that an incident of this nature happens every seven minutes. Misbehavior has been known to target children through virtual world chat messages or by hackers speaking to them through headsets, incidents that are difficult to document.

Companies have a legal obligation to provide employees and consumers with a safe working environment and to protect them from the bad behavior of others. It begins with companies updating their policies to consider these different forms of harassment.

Companies must improve their platforms to report misbehavior easily and implement mechanisms to track incidents in real-time, and resolve all incidents that occur internally or through external means. Despite this bad behavior, many individuals and companies are working to make the Metaverse safe for everyone.

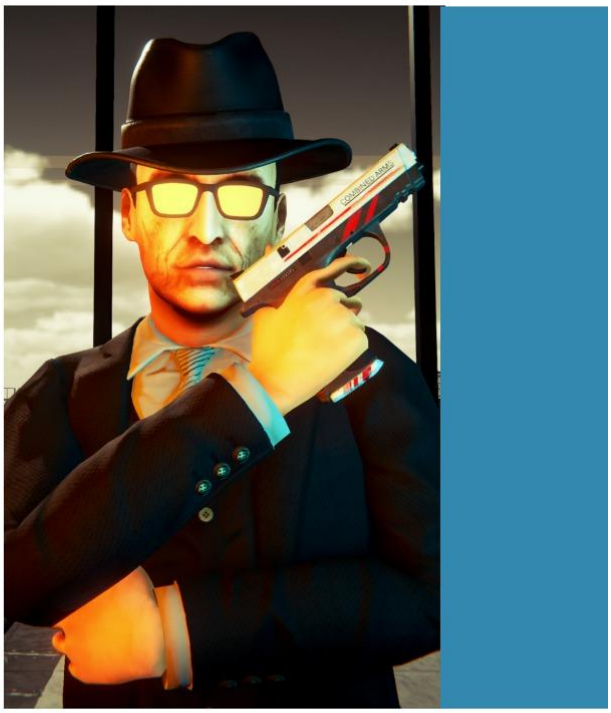
Financial Crimes

Companies that have entered the Metaverse face a major new financial crime challenge as the old rules for achieving trust in your transactions, assets, data, and brand experience no longer apply. Virtual worlds with 3D avatars permit individuals to be anonymous, causing havoc to financial market regulations like AML and KYC. The key aspect of virtual worlds is the decentralization usage of the blockchain thwarting crypto-based crimes, and crypto-enabled criminal networks are much more difficult for authorities to monitor and detect these crimes.

Recently, Interpol conducting an operation in thirty countries, uncovered illicit fund movement across borders using these virtual worlds by scammers and fraudsters. Financial Crimes identified in these virtual worlds by investigators include identity theft, where an individual exchanges a digital asset for a name, date of birth, and a driver's license. This virtual purchase of real-world Personal Identifiable Information ("PII") is then used for credit-card fraud, bank fraud, or whatever crime you can think of using PII. Ever wonder how a company can measure credit risk without credit reports? Without a background check, PII can also be used to acquire a legal firearm. Criminal investigators have also observed human trafficking and money laundering used for terrorism.

Terrorist organizations have also used these virtual worlds for propaganda, recruitment, and training. Moreover, an accurate and complete virtual world can be used for military reconnaissance and planning.

Hackers and criminals have been known to use the metaverse to more convincingly impersonate individuals and brands, lulling others into a false sense of security that sharing their personal information is safe. Suppose your customers are entrusting you with financial assets. In that case, companies need both special protocols to protect the customers and procedures to make them whole if they suffer an incident or financial crime within your virtual world. Companies must update their security and incident playbook for the Metaverse.



Conclusion

The Metaverse presents a host of risks for clients and companies, even if they are experimenting with it. As companies migrate to this new virtual environment, they must take a hard look at the material risks they encounter and how to monetize the user experiences safely. Companies in the Metaverse will need new rules to govern security, interactions among users, tax collection, data governance, regulatory compliance, and more. Companies should also consider engaging with regulators to help shape the metaverse rules of the road.

A big responsibility that will fall on companies is to monitor and moderate what happens on their platforms and provide law enforcement with incident logs to resolve their bad behaviors. As with current online activities, this will be challenging and only amplified and exacerbated with new issues to overcome.

Customers must understand the risks they will encounter in the Metaverse by asking how their data is being collected and used as well as the security of their data. Customers should also press the companies on incident response and ensure the virtual world they play in is properly policed by the host.

breakroom sinespace

Thank You

SINE WAVE ENTERTAINMENT

With 15 years of experience, Sine Wave Entertainment is revolutionizing Metaverse innovation by creating a virtual world where users have an equal digital representation. We're passionate about building real-world paradigms that strongly adhere to the principles of diversity and inclusion - ushering in a new era for online experiences!

CONTACT US :

+44 20 8144 1418
Contact@sinewavecompany.com
www.breakroom.net

OUR OFFICE :

48 Dover Street
London, W1S 4FF
United Kingdom

For more information or to book a personal tour visit:

www.breakroom.net