Bloomberg Law

Insuring the Metaverse: New Worlds Meet Old Policies

April 8, 2022

Covington & Burling LLP attorneys suggest how the insurance industry might respond to the unique risks that are sure to arise from commerce in the metaverse. Coverage issues may sound esoteric to anyone outside a corporate risk management office, but the money at stake—which could be billions—should be top-of-mind in the C-suite, they say.

Businesses are investing real money in virtual assets. They are buying property on metaverse platforms, selling branded digital goods in the metaverse, and investing in elaborate virtual user experiences. Are potential losses and liabilities that may arise from the development and use of metaverse digital assets covered by insurance?

This question may sound esoteric to anyone outside a corporate risk management office, but the money at stake (which could be billions) should be top-of-mind within the C-Suite.

Novel risks are sure to arise from metaverse commerce. Current commercial insurance products might respond in a number of different ways.

It's the Same, But Different

The general types of losses and liabilities arising from the metaverse will likely resemble those companies now face because of internet and social media activities: hacking, business interruptions, privacy breaches, and ransomware attacks.

What will differ, however, is how much time we will spend in the metaverse—working, socializing, buying, selling, dating, gaming, sharing religious observances, and celebrating life events.

For those whose metaverse identity becomes their primary identity, the loss or destruction of essential elements of that virtual identity could seem catastrophic. Faced with angry consumers and large claims or remediation costs, a business will want to know which of its insurance assets will respond and whether its current insurance portfolio contains coverage gaps.

Cyber Coverage, a First Place to Look—Carefully

Cyber insurance is the most likely source of protection for risks arising from metaverse commerce. Cyber policy forms vary, but they typically cover a variety of third-party liabilities and first-party losses related to data/network security and privacy events, including consumer liability claims for unauthorized collection or disclosure of private information, government investigations and regulatory proceedings, business interruption, data restoration, and ransomware attacks.

While cyber policies do not (yet) reference the metaverse specifically, their coverage should extend generally to the digital and data risks that arise from commerce in the metaverse.

But cyber policies can be full of traps for the unwary. For example, depending on how the policy defines key terms such as "Computer System," it might cover third-party claims and first-party losses involving your owned or controlled computer system, and your contracted cloud providers' —but not those arising from servers outside your or your direct vendors' ownership or control.

Also, while cyber policies often cover data restoration services, many do not insure a data asset's reduced market value.

For example, imagine that a consumer products business creates a branded store on prime metaverse real estate, it becomes the target of cyber vandalism or a ransomware attack, and it must be taken off line for some time. A typical cyber policy should cover the costs of restoring the data to its original state, ransom payments, and business interruption losses. But if the market value of the virtual store when restored has plummeted, coverage may be disputed unless the cyber policy's terms have been tailored to address that novel risk.

Policyholders with metaverse exposures should approach the underwriting process with a clear understanding of those risks, how they might fall through the cracks of standard policy wordings, and alternative wordings that could restore coverage.

Beware of Efforts to Silence 'Silent Cyber'

"Silent cyber" is the insurance industry's term for coverage afforded to cyber-related risks under traditional standard-form first-party property/business interruption and third-party liability policies.

Insurers view such coverage as "silent" because these policies do not expressly reference cyber-related exposures, but their "all risks" or "comprehensive" coverage grants, absent specific exclusions, are often broad enough to cover physical injuries caused by cyber-related perils.

With the digital and physical worlds increasingly overlapping, however, insurers are increasingly adding cyber exclusions to traditional policies in an apparent effort to place "physical" and "cyber" risks in separate coverage silos. But coverage gaps may lie between those silos. Without care at the underwriting stage, your metaverse claim could get lost in space.

What About Traditional Liability Policies?

The traditional commercial general liability (CGL) policy should continue to cover bodily injury and property damage claims involving tangible, non-electronic property, provided the insurer has not introduced exclusions for cyber-related risks.

For instance, barring such exclusions, claims that an individual has developed headaches and other physical ailments due to the immersive aspects of the metaverse should be covered, but an insurer would contest coverage for purely mental injury or damage only to electronic data.

CGL policies also cover enumerated offenses like defamation, invasion of privacy, and disparagement that might occur in the metaverse.

What If It's the Same Loss, But in the Metaverse?

Standard commercial insurance policies currently do not exclude claims merely because they arise in the metaverse. Thus, policies covering certain types of claims arising outside the metaverse should cover the same types of claims arising within it.

Employers practices liability policies should continue to cover employment-related claims such as discrimination and harassment, even if occurring outside the physical office and in the virtual office.

Errors and omissions policies should continue to cover liability for service errors within the metaverse.

Directors and officers policies should continue to cover metaverse-related liability claims, including securities investigations and claims against directors and officers.

But insurers' increased concerns over "silent cyber" may prompt them to try to reduce coverage. Insurance buyers will need increased expertise to ensure seamless metaverse-related protection. When the real and virtual worlds converge, insurance can get tricky.

This article does not necessarily reflect the opinion of The Bureau of National Affairs, Inc., the publisher of Bloomberg Law and Bloomberg Tax, or its owners.

Author Information

Georgia Kazakis is a partner with Covington & Burling LLP in Washington, D.C., with extensive experience representing policyholders in complex insurance coverage matters, including emerging areas like those involving artificial intelligence.

Stuart Irvin is of counsel with Covington in Washington, D.C., and founder of the firm's Video Games and Esports practice.

Scott Levitt is special counsel with Covington in Washington, D.C., with over 25 years of experience representing policyholders in numerous types of insurance coverage claims.

John Buchanan is senior counsel with Covington in Washington, D.C., with over three decades of experience representing policyholders, including cyber-related and other emerging insurance coverage issues.