The advent and impending buildout of the Metaverse will fundamentally alter investment opportunities in several industries, including retail, cybersecurity, and healthcare. In each of these sectors, we believe novel virtual technologies will enhance customer satisfaction, unlock growth levers that expand addressable markets, and catalyze profit margin expansion.

We believe the Metaverse revolution will be particularly impactful on the luxury goods segment within the retail industry, providing enablement opportunities for both physical commerce and sales of virtual goods. Early iterations of augmented reality (AR) are already transforming the purchasing process, as retailers increasingly partner with technology leaders to optimize consumer experiences. For example, Snapchat users can try on clothing, bags and other accessories with AR technology that detects and responds to body movements and facial dimensions. Snapchat, which added Farfetch and Prada to its roster of luxury goods partners in early 2021, also facilitates product catalogue integrations, virtual changing rooms, and the ability for users to shop for items seen in real life.[1] According to Shopify, merchants who integrate AR and 3D content experience a 94 percent increase in conversion rates.[2] Based on this trend, tech-enablement will drive demand and expand addressable markets for retail by empowering consumers to seamlessly test out products and interact with their social networks.

The current retail and e-commerce industry is fraught with frictions, inefficiencies, and consumer dissatisfaction. According to the National Retail Federation, American consumers returned $428 billion in merchandise in 2020, including $102 billion of merchandise purchased online.[3] In the case of online purchases, it is difficult for consumers to gauge the sizing and aesthetic of purchased goods, driving outsized return rates for e-commerce. Fraudulent returns also produce major headaches for retailers. The NRF estimates that retailers lose $5.90 to fraud for every $100 in returned merchandise accepted, representing a sizeable hit to profit margins. However, the Metaverse can induce a major paradigm shift, allowing users to "try on" clothing and accessories in computer-generated fitting rooms from the comfort of their homes. This will fundamentally improve consumer satisfaction and decrease return rates, generating operational efficiencies and increasing margins for retailers.

In addition to augmenting purchasing decisions for physical luxury goods, the Metaverse can also facilitate luxury goods manufacturers with opportunities to further monetize intellectual property as non-fungible token collectibles (NFTs). Digital avatars will inevitably require clothing and accessories that establish distinct personal identities. Analogous to our physical reality, individuals participating in virtual worlds can leverage elite trademark-protected brands as displays of wealth, exclusivity, and social know how.

Blockbuster games like Fortnite have already established the necessary precedent for sales of virtual luxury goods by allowing users to purchase augmentative 'skins.' In addition, Nike recently announced a partnership with Roblox to build "Nikeworld" within the online gaming platform, incorporating Nike-branded arenas for mini-games and virtual apparel for avatars.[4] This partnership has the potential to drive both virtual and physical sales of Nike's products, ultimately providing a crossover framework for luxury goods companies operating in the Metaverse. Morgan Stanley estimates that Metaverse gaming and NFTs could represent a $56 billion opportunity for the luxury market by 2030, expanding the luxury goods total addressable market by 10% and growing industry profitability (EBIT) by 25%.[5] Notably, the analysts highlight that the Metaverse will allow luxury goods companies to appeal to a broader audience, particularly younger male customers.

Although the luxury NFT industry remains in the nascent 'early adopter' phase, we are rapidly approaching an inflection point. In September, renowned Italian fashion house Dolce & Gabbana sold its nine-piece NFT "Genesis" collection for the equivalent of $5.7 million in Ethereum, a landmark sale that marks the beginning of a wave of NFT sales for all luxury goods vendors.[6] LVMH, owner of the acclaimed Louis Vuitton and Dior brands, and Kering, Gucci's parent company, are particularly well-positioned to capitalize on this emerging 'retail' economy. These established luxury conglomerates have the requisite experience managing scarcity and implementing effective pricing strategies.

In addition to generating tailwinds for the retail industry, inflecting growth in virtual reality (VR) utilization will necessitate heavy investment in "zero trust" cybersecurity, particularly in the subsegments of identity, endpoint, and cloud security. Criminal organizations and nation-state hackers do not discriminate, targeting critical data and information wherever it is being held. Malicious actors capitalized on widespread security inadequacies that emerged during the distributed work-from-home environment in 2020, as malware increased by 358 percent and ransomware increased by 435 percent year-over-year.[7] VR will obviously magnify this problem. As more applications, consumer information, and financial data transition to the Metaverse, cyber-attacks will most likely proliferate and pose major risks to enterprises and consumers alike.

[1]McDowell, Maghan, and Kati Chitrakorn. "Snapchat Boosts Ar Try-on Tools: Farfetch, Prada Dive In." Vogue Business, 21 May 2021, https://www.voguebusiness.com/technology/snapchat-boosts-ar-try-on-tools-farfetch-prada-dive-in.
[2]Wynne Lockhart, Jessica. "How Augmented Reality (AR) Is Changing Ecommerce Shopping as We Know It." Shopify Plus, 29 Sept. 2021, https://www.shopify.com/enterprise/augmented-reality-ecommerce-shopping.
[3]Inman, Danielle, et al. "$428 Billion in Merchandise Returned in 2020." NRF, 11 Jan. 2021, https://nrf.com/media-center/press-releases/428-billion-merchandise-returned-2020.
[4]Golden, Jessica. "Nike Teams up with Roblox to Create a Virtual World Called Nikeland." CNBC, 19 Nov. 2021, https://www.cnbc.com/2021/11/18/nike-teams-up-with-roblox-to-create-a-virtual-world-called-nikeland-.html.
[5]Canny, Will. "Metaverse Gaming, Nfts Could Account for 10% of Luxury Market by 2030: Morgan Stanley." CoinDesk Latest Headlines, Morgan Stanley, 22 Nov. 2021, https://www.coindesk.com/business/2021/11/22/metaverse-gaming-nfts-could-account-for-10-of-luxury-market-by-2030-morgan-stanley/.
[6]Thomas, Dana. "Dolce & Gabbana Just Set a $6 Million Record for Fashion Nfts." The New York Times, The New York Times, 4 Oct. 2021, https://www.nytimes.com/2021/10/04/style/dolce-gabbana-nft.html.
[7]Deep Instinct. "Malware Increased by 358% in 2020." Help Net Security, Deep Instinct, 17 Feb. 2021, https://www.helpnetsecurity.com/2021/02/17/malware-2020/.

As enterprises increasingly shift workflows and meetings to VR environments such as Facebook's 'Horizon Workrooms,' it will become more important than ever to verify identities with multi-factor authentication, manage employee access to sensitive applications and data, and establish robust compliance policies. Best-of-breed, technology-agnostic, and SaaS-based identity vendors are best positioned to adapt security technology and policy frameworks to successfully protect enterprises' Metaverse technology assets.

Endpoint security will also become critical for protecting the hardware assets that enable employees and consumers to enter virtual worlds. Cloud-native, next-generation antivirus (NGAV) software, will become critical for protecting internet-connected VR headsets. Endpoint security software companies deploy AI-powered lightweight agents that help to protect against both known and unknown ("zero day") malware infections using predictive capabilities. Core malware protections include sandboxing, program termination, and data loss prevention (DLP). As VR headsets become mainstream, malicious developers will increasingly divert their efforts to develop malware specifically targeting VR operating systems. Headset malware infections can result in data theft, corporate embarrassment, and subsequent blackmail and ransom payments. As the NGAV market for PCs and mobile phones becomes increasingly saturated, security protection for VR headsets and other Metaverse IoT devices represents what we believe is an underappreciated growth driver.

Demand for cloud security software will accelerate as the development of technology applications can generate a massive expansion in the consumption of public cloud computing and infrastructure services. As an illustration of this point, Meta (formerly Facebook) recently deepened its relationship with Amazon Web Services to "scale research and development, facilitate third party collaborations, and drive operational efficiency."[8]

In order for the Metaverse to properly function, the integrity of data centers, servers, and networks must be secured by cloud security software. Cloud security software enables companies to "secure infrastructure, applications, and data across hybrid and multi-cloud environments."[9] Key components of cloud security include cloud workload protection (CWP), virtual firewalls that provide traffic packet inspection and other network security functionality, and cloud security posture management (CSPM) to provide compliance teams with access policy visibility. Leading vendors in this emerging industry include CrowdStrike, legacy network security providers like Palo Alto Networks, and content-delivery network (CDN) vendors like Cloudflare.

In consequence of growing AR and VR applications, the healthcare industry is ripe for technological disruption in areas including medical training, surgery, and telehealth. For example, the World Health Organization developed an AR smartphone simulation that demonstrates the proper techniques for putting on and removing personal protective equipment to fight the COVID pandemic.[10] Furthermore, UConn Health is training orthopedic surgery residents using Meta's Oculus technology. These virtual training environments allow students to make mistakes, receive feedback from faculty, and incorporate improvements into their subsequent "operations." The healthcare educational opportunities are vast, and software application developers are poised to capture significant economic value.

Regarding telehealth, the Metaverse can be a major secular driver of patient adoption, utilization, and engagement with major platforms. These platforms can develop applications on Oculus and other VR platforms that enable "face-to-face" meetings between physicians and patients, facilitating a stronger emotional connection than that over phone or video. Despite the elevated level of telehealth adoption achieved during the COVID-19 pandemic, one survey of 2,080 patients found that the majority (53.0%) of patients still prefer in-person visits.[11] Evidently, patients crave interpersonal interaction to provide them with a sense of security about their health. Telehealth adoption within virtual environments, combined with increased at-home diagnostic device adoption, can improve clinical outcomes and consumer satisfaction. Major platforms may experience accelerating growth and profit margin expansion should further economies of scale develop.

Nels Wangensteen
Co-Founder, Portfolio Manager

Ingrid Yin, Ph.D.
Co-Founder, Portfolio Manager

Alexander Brett
Equity Research Associate

[8]"Meta Selects AWS as Key, Long-Term Strategic Cloud Provider." Amazon.com, Inc. - Press Room, 1 Dec. 2021, https://press.aboutamazon.com/news-releases/news-release-details/meta-selects-aws-key-long-term-strategic-cloud-provider.
[9]"Prisma Cloud: Comprehensive Cloud Security." Palo Alto Networks, https://www.paloaltonetworks.com/prisma/cloud.
[10] Woods, Bob. "The First Metaverse Experiments? Look to What's Already Happening in Medicine." CNBC, 4 Dec. 2021, https://www.cnbc.com/2021/12/04/the-first-metaverse-experiments-look-to-whats-happening-in-medicine.html.
[11]S. Predmore, Zachary. "Assessment of Preferences for Telehealth in Post–COVID-19 Health Care." JAMA Network Open, JAMA Network, 1 Dec. 2021, https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2786700.

Disclaimers:

The opinions expressed herein represent the views of management (or investment professionals) based on market conditions as of the date of this publication and may change at any time without notice. We assume no obligation to provide an update to this article. Recipients are advised not to infer or assume that any securities, strategies, companies, sectors or markets described will be profitable or that losses will not occur. It should not be assumed that recommendations made in the future will be profitable or will equal the performance of the securities in this list. This article includes information from third party sources believed to be reliable; however, we make no representation as to its accuracy or completeness.

The materials do not purport to contain all of the information that may be required to evaluate the investment strategy, or a portfolio and you should conduct your own independent analysis of the presentation. Any decision to invest in securities or strategies described herein should be made after reviewing the Firm's Form ADV Part 2A, conducting such investigation as an investor deems necessary and consulting its own legal, accounting and tax advisors to make an independent determination of suitability and consequences of such an investment. References to any specific investments, strategies or investment vehicles are for illustrative purposes only and should not be relied upon as recommendation to purchase or sell such investments or to engage in any particular strategy. The investment strategy and themes discussed herein entail a high degree of risk and may not be suitable for investors depending on their specific investment objectives and financial situation. Investing in securities represents the risk of a partial or total loss of your investment.

Securities mentioned in this article that MayTech has purchased and currently owns in its client accounts and/or employees' personal accounts:

Security Name	Position Type	Initial Date	Initial Purchase Price*	Market Price as of 1/11/2022
Amazon Inc.	Long/Buy	8/18/2009	169.35	3307.24
Meta Platforms, Inc	Long/Buy	1/26/2016	97.25	334.37
Palo Alto Networks	Long/Buy	10/12/2021	507.38	526.05
Tencent Holdings	Long/Buy	8/27/2009	14.59	59.01
LVMH	Long/Buy	8/8/2019	406.46	814.28
Crowdstrike	Long/Buy	1/6/2022	183.06	196.11

*Initial purchase indicated pre stock split (where applicable) and may not be compared to current market price to gauge performance.

FOR A COMPLETE LIST OF MAYTECH'S HOLDINGS PLEASE CONTACT COMPLIANCE@MAYTECHGLOBAL.COM