Risk Factors Comparison 2025-05-15 to 2024-05-16 Form: 10-K

Legend: **New Text** ~~Removed Text~~ Unchanged Text Moved Text Section

We are subject to a number of risks that, if realized, could materially and adversely affect our business, financial condition, results of operations, and cash flows and our ability to make distributions to our stockholders. Some of our more significant challenges and risks include, but are not limited to, the following, which are described in greater detail below: • If we are unable to develop new and enhanced solutions and products, or if we are unable to continually improve the performance, features, and reliability of our existing solutions and products, our business and operating results could be adversely affected. • We operate in a highly competitive and dynamic environment, and if we are unable to compete effectively, we could experience a loss in market share and a reduction in revenue. • Issues in the development and deployment of artificial intelligence (" AI ") may result in reputational harm and legal liability and could adversely affect our results of operations. • Our acquisitions and divestitures create special risks and challenges that could adversely affect our financial results. • Our revenue and operating results depend significantly on our ability to retain our existing customers and expand sales to them, convert existing non- paying customers to paying customers and add new customers. • If we fail to manage our sales and distribution channels effectively, if our partners choose not to market and sell our solutions to their customers, or if we have an adverse change in our relationships with key third- party partners, service providers or vendors, our operating results could be materially and adversely affected. • Changes in industry structure and market conditions have and may continue to lead to charges related to discontinuance of certain of our products or businesses and asset impairments. • Our international operations involve risks that could increase our expenses, adversely affect our operating results and require increased time and attention of our management. • Our future success depends on our ability to attract and retain personnel in a competitive marketplace. • If the information provided to us by customers or other third parties is incorrect or fraudulent, we may misjudge a customer' s qualifications to receive our products and services and our results of operations may be harmed and could subject us to regulatory scrutiny or penalties. • Our solutions, systems, websites and the data on these sources have been in the past and may continue to be subject to cybersecurity events that could materially harm our reputation and future sales. • We collect, use, disclose, store or otherwise process personal information and other sensitive data, which is subject to stringent and changing state and federal laws and regulations. • Our inability to successfully recover from a disaster or other business continuity event could impair our ability to deliver our products and services, which could harm our business. • We are dependent upon Broadcom for certain engineering and threat response services, which are critical to many of our products and business. • If we fail to offer high- quality customer support, our customer satisfaction may suffer and have a negative impact on our business and reputation. • Our solutions are complex and operate in a wide variety of environments, systems and configurations, which could result in failures of our solutions to function as designed. • Negative publicity regarding our brand, solutions and business could harm our competitive position. • Our reputation and / or business could be negatively impacted by sustainability and governance matters and / or our reporting of such matters. • We are affected by seasonality, which may impact our revenue and results of operations. • Our solutions are highly regulated and the legal and regulatory regimes governing certain of our products and services are uncertain and evolving, which could impede our ability to market and provide our solutions or adversely affect our business, financial position and results of operations. • The regulatory regime governing blockchain technologies and digital assets is uncertain, and new laws, regulations or policies, including licensing laws, may alter our business practices with respect to digital assets. • If we do not protect our proprietary information and prevent third parties from making unauthorized use of our products and technology, our financial results could be harmed. • From time to time we are party to lawsuits and investigations which has previously and could in the future require significant management time and attention, cause us to incur significant legal expenses and prevent us from selling our products. • Third parties have claimed and additional third parties in the future may claim that we infringe their proprietary rights. • Some of our products contain " open source " software, and any failure to comply with the terms of one or more of these open source licenses could negatively affect our business. • There are risks associated with our outstanding and future indebtedness that could adversely affect our financial condition. • Our Amended Credit Agreement imposes operating and financial restrictions on us. • We may be unsuccessful in managing the effects of changes in the cost of capital on our business. • The failure of financial institutions or transactional counterparties could adversely affect our current and projected business operations and our financial condition and result of operations. • If our existing funding arrangements are not renewed or replaced or our existing funding sources are unwilling or unable to provide funding to us on terms acceptable to us, or at all, it could have a material adverse effect on our business, financial condition, results of operations and cash flows. • Hedging or other mitigation actions to mitigate against interest rate exposure may adversely affect our earnings, limit our gains or result in losses, which could adversely affect cash available for distributions. • Adverse macroeconomic conditions and government efforts to combat inflation, along with other interest rate pressures, have led to and may continue to lead to higher financing costs and may particularly have negative effects on the consumer finance industry and our MoneyLion business. • Fluctuations in our quarterly financial results have affected the trading price of our stock in the past and could affect the trading price of our stock in the future. • We may be required to issue shares under our contingent value rights agreement with certain former holders. • Changes to our effective tax rate could increase our income tax expense and reduce (increase) our net income (loss), cash flows and

working capital and audits by tax authorities could result in additional tax payments for prior periods. • We could be obligated to pay additional taxes in various jurisdiction, which would harm our results of operations. • Our ability to use our deferred tax assets to offset future taxable income may be limited. The above list is not exhaustive, and we face additional challenges and risks. Please carefully consider all of the information in this Annual Report on Form 10- K, including the matters set forth below in this Part I, Item 1A. PART I Item 1. Business Purpose and Mission Purpose: Powering Digital Freedom. Mission: We create innovative and easy- to- use technology solutions that help people grow, manage and secure their digital and financial lives. Our Values Protecting people is what inspires us, and our people are at the core of what we do. We seek to attract talent that embraces the following values: • Customer Driven. Community Minded. We are customer obsessed and drive positive impact. • Think Big. Be Bold. We embrace change and innovate fearlessly. • Be Scrappy. Make it Happen. Big or small, we get things done irrespective of title or role. • Play to Win. Together. We win for our customers, with passion and integrity. Company Overview Gen is a global company powering Digital Freedom with a family of trusted brands including Norton, Avast, LifeLock and more. We bring award- winning products and services in cyber safety, covering security, privacy, identity protection and financial wellness to approximately 500 million users in more than 150 countries, empowering them to live their digital lives safely, privately, and confidently today and for generations to come. Today' s world is increasingly digital, and this has changed the way we live our lives every day. The last decade has brought increasingly impressive technological advances that have unlocked new ways to play and transact online, control smart homes, manage our life and more. The possibilities in the digital world will continue to unlock new possibilities. However, as our digital footprint expands, so do the risks and exposure. Cybercriminals use a mix of old and new tactics and technologies, including phishing, vishing, smishing, based on machine learning and generative artificial intelligence (AI) technologies, to execute highly advanced threats and attacks. We are our customers' trusted ally that they can depend on to help secure and control their digital lives so they can be free to enjoy the promise of the digital world. We are committed more than ever to protecting and empowering people' s digital lives with personalized, human- centered safety. We are well- positioned to drive awareness of cyber safety for individuals, families, and small businesses, fueled by an increasingly connected world. We maintain a global, omni- channel sales approach, including direct, indirect and freemium acquisition and a family of brands marketing program. This program is designed to grow our customer base by increasing brand awareness and understanding of our products and services and maximizing our global reach to prospective customers. We help prevent, detect and restore potential damages caused by cybercriminals. We also make it easy for consumers to find, buy and use our products and services. To this end, we offer both free and paid subscription- based cyber safety solutions primarily direct- to- consumer through our family of brands and indirectly through partner relationships. Most of our subscriptions are offered on annual terms, but we also provide monthly subscriptions. As of March 28, 2025, we have approximately 500 million total users, which come from direct, indirect and freemium channels. Of these total users, we have approximately 65 million paid cyber safety customers including over 40 million direct customers with whom we have a direct billing relationship. • Direct- to- consumer channel: We use advertising to elevate our family of brands, attract new customers and generate significant demand for our services. Our direct subscriptions are primarily sold through our e- commerce platform and mobile apps, and we have a direct billing relationship with the majority of these customers. • Indirect partner distribution channels: We use strategic and affiliate partner distribution channels to refer prospective customers to us and expand our reach to our partners' and affiliates' customer bases. We developed and implemented a global partner sales organization that targets new, as well as existing, partners to enhance our partner distribution channels. These channels include retailers, telecom service providers, hardware original equipment manufacturers (OEMs), employee benefit providers, strategic partners, small offices, home offices and very small businesses. Physical retail and OEM partners represent a small portion of our distribution, which minimizes the impact of supply chain disruptions. • Freemium channels: With the acquisitions of Avast and Avira, we have expanded our go- to- market with multiple freemium channels. We use free versions of our products to reach the broadest set of consumers globally and bring cyber safety to a larger audience, especially in international markets. The free solution offers a baseline of protection and presents premium functionalities based on the risk profile and specific needs of the user. The user can choose to add specific premium solutions or upgrade to suites that provide security, identity, and privacy across multiple platforms and devices, thereby becoming a paid customer. Seasonality As is typical for many consumer technology companies, portions of our business are impacted by seasonality. However, we believe the net impact on our business is limited. Seasonal behavior in orders primarily reflects consumer spending patterns during our fiscal third and fourth quarters, as order volume is generally higher due to the holidays in our third quarter, as well as due to follow- on holiday purchases and the U. S. tax filing season which is in our fourth quarter. Revenue generally reflects similar seasonal patterns but to a lesser extent than orders because of our subscription business model, as the majority of our in- period revenues are recognized ratably from our deferred revenue balance. Our Strategy Our strategy is focused on long- term profitable growth. To fuel our growth, our consumer- centric strategy is to provide comprehensive and easy- to- use integrated platforms, which we have built in- house or acquired. By combining and leveraging our family of trusted consumer brands, including offerings from Norton, Avast, LifeLock and more, we deliver an industry- leading cyber safety and trust- based solutions. We are positioned for long- term growth and expansion. Our three primary growth levers are: 1. Extending Reach: Leveraging an omni- channel strategy and building partnerships to broaden privacy and identity protection internationally. 2. Increasing Value: Cross- selling and up- selling, and expanding security, identity and privacy solutions to address consumers' evolving needs. 3. Growing Loyalty: Increase customer loyalty and retention, as consumers move from point products protecting their devices towards all- in- one comprehensive cyber safety memberships. The key elements of our strategy include the following: •

Extend our leadership position through new products and continued enhancement of our trust- based solutions and services: Cyber safety is a large and expanding market, which we believe provides a significant growth opportunity. Our strategy is to grow our business through innovation and acquisitions to expand the solutions and services we offer into new cohorts, territories and sectors. We believe there are many additional areas where we can both offer new solutions, as well as use our core capabilities and our integrated platform to reach new customers and markets globally. • Grow our customer base through multiple channels: We have multiple go- to- market channels to reach new customers globally, including direct- to- customer, indirect partnerships and freemium. We intend to leverage our expertise in digital marketing, as well as existing and new strategic partnerships, to grow our customer base. We believe that continued investments in these areas, as well as our product offerings and infrastructure, will allow us to further enhance our leading brands and superior products, increase awareness of our consumer services and enhance our ability to efficiently acquire new customers. • Continue our focus on customer retention: We continue to optimize and expand the value we provide to customers which we believe can positively impact retention. We aim to continue to increase customer engagements through actionable alerts, education on timely topics and introducing new product capabilities. We also plan to continue investing in enhancing both desktop and mobile customer experiences throughout a customer' s journey with Gen, from purchase, to onboarding and beyond. • Increase value to existing customers: We believe strong customer satisfaction will provide us with the opportunity to engage customers in new services offerings. We maintain the Norton 360 and Avast One platforms that have multiple tiers of membership, and we continue to engage customers with standalone products to offer membership options and show the value proposition of our premium solutions. Over time, we plan to drive further growth as we add additional offerings and services for our customers. • Draw strength from our world- class customer service support: Our global support team seeks to ensure the voice of the consumer is heard and that we put our customers first. We leverage frequent communication and feedback from our customers to continually improve our solutions and services. We embrace end- to- end customer experience and aim to continue to improve our Net Promoter Scores and overall customer satisfaction. • Leverage our global brands to drive growth: We will work to keep building our family of trusted brands in markets globally as we strive to bring protection and empowerment to all consumers when it comes to their digital lives. According to our most recent research, Norton has 93 % global brand awareness, and we are best positioned and top of mind in consumer cyber safety, according to the internal H1 2025 Gen Brand Tracker. Our Cyber Safety Solutions and Services Our broad portfolio of products and services is developed from consumer insights to help us bring to market real solutions to real problems and to engage and educate consumers about cyber safety. We continuously aim to release new products and features to outpace evolving threats and find synergies to integrate current and future technology acquisitions. Our cyber safety portfolio provides protection across three key categories in multiple channels and geographies, including security and performance, identity protection, and online privacy. Leveraging our technology platforms, we integrate software and service capabilities within these three categories into comprehensive and easy- to- use products and solutions across our brands. We have also evolved beyond traditional cyber safety to offer adjacent trust- based solutions, including digital identity and access management, digital reputation, and restoration support services. We protect and empower consumers by providing solutions and services in two main ways: • Comprehensive membership plans: Providing a comprehensive and all- in- one cyber safety portfolio of solutions for a membership fee. Plans are offered through Norton 360 and Avast One subscriptions, with both brands providing multiple levels of membership tiers that range from basic, mid- level, or premium tiers where identity theft and online privacy features are included. • Point solutions: Providing individual, stand- alone products and services in security, identity and privacy, offering flexibility for consumers to choose between free or paid solutions. These products solve for a specific need, when you need it, and can add on to the value you already have. Please see below for our full set of products by category. We are well positioned across three key cyber safety categories: • Security and Performance (Norton, Avast, Avira, AVG, and CCleaner offerings): Our offerings provide real- time threat protection for PCs, Macs and mobile devices against malware, viruses, adware, ransomware and other online emerging threats. These offerings monitor and block unauthorized traffic from the internet to the device to help protect private and sensitive information when customers are online. Additionally, our all- in- one cybersecurity solutions help small business owners safeguard their team' s online activities, devices and customer data. Scams have also continued to become more prevalent and sophisticated and we offer a range of AI-powered features integrated into Norton Cyber Safety products to provide always- on protection from today' s most sophisticated scams across phone calls, texts, emails, and websites. Norton Scam Protection and Scam Protection Pro utilize Norton Genie AI engine to analyze the meaning of words, not just links, helping to stop hidden scam patterns that even the most careful person can miss. We also provide performance and optimization software solutions that free up space on devices, clear online tracking and help machines run faster. • Identity Protection (U. S.: LifeLock Identity Theft Protection, Avast and AVG Secure Identity; International: Norton Identity Theft Protection, Dark Web Monitoring): In the U. S., we offer Identity Theft protection as part of our LifeLock, Avast and AVG brands. All three products include monitoring of credit reports, the dark web and social media accounts to help safeguard our customers' personal information. The LifeLock product also offers monitoring of financial accounts. In the event of identity theft, we assign an Identity Restoration Specialist to work directly with customers to help restore their identities, and all plans include reimbursements for losses and expenses incurred ranging up to $ 3 million. Outside the U. S., we offer Norton and have expanded Avast and AVG branded plans to additional regions. Plans include dark web monitoring in over 50 countries and monitoring of credit, social media and financial accounts, restoration support and identity theft insurance in select countries. • Online Privacy (VPN, multiple personal data protection products, ReputationDefender): Our virtual private network (VPN) solutions offered through the Norton, Avast and AVG brands enhance security and online privacy by

providing an encrypted data tunnel. This allows customers to securely transmit and access private information, such as passwords, bank details and credit card numbers, when using public Wi- Fi on PCs, Macs, and mobile iOS and Android devices. We offer a variety of solutions under the Norton and Avast brands to protect customers' data either by keeping data anonymous while browsing online through our AntiTrack and Secure Browser products or helping customers remove data from public data broker sites through our Privacy Monitor Assistant and BreachGuard products. Norton offers a three- tiered VPN with advanced privacy and malware protection as well as AI- powered protection against sophisticated cyber threats, including scams and phishing attacks. ReputationDefender is a white glove service that helps customers manage all aspects of their personal branding online, including search results, social media sites and overall web presence. Innovation, Research and Development Gen has a long history of innovation, and we plan to continue to invest in research and development to drive our long- term success. As cyber threats evolve, we are focused on delivering a portfolio that protects each element of our customers' digital lives. To do this, we engage and listen to our customers, and we embrace innovation by deploying a global research and development strategy across our cyber safety platform. Our engineering and product management teams are focused on delivering new versions of existing offerings, as well as developing entirely new offerings to drive the company' s global leadership in cyber safety. We are committed to our innovation and research and development efforts. The Technology team at Gen is driving the company' s future technologies and innovation and helping guide the consumer cybersecurity industry. Our global technology research organization is focused on applied research projects, with the goal of rapidly creating new products to address consumer trends and grow the business, including defending consumer digital privacy and identity. We also have a global threat response and security technology organization that is comprised of our dedicated team of threat and security researchers, supported by advanced systems to innovate security technology and threat intelligence. We have one of the world' s largest consumer cyber safety networks. Leveraging our capabilities, our global threat response team handles a wide variety of attacks, including social engineering attacks, file- based attacks, web and network- based attacks, privacy and data exfiltration attacks, identity theft attacks, algorithmic manipulation attacks, and more. Our differentiated approach is powered by our global scale and visibility, geographically distributed cloud data platform, and advanced AI- based automation. Industry Overview Cyber safety is a growing market, fueled by the increase in activities online over the years as well as expected growth in the years ahead. The core markets that we participate in are security, identity and privacy. We believe the cyber safety market will continue to expand beyond these core markets and grow significantly, driven by the increasing number of people globally connected to the internet and their expanding digital lives. The cyber threat landscape is larger and more complicated than ever before, exposing consumers to an increased risk to their digital lives. The digitization of the world and the overlap between the physical and digital world are growing at a fast pace. New technologies, smart devices, digital identities and an increasingly more connected world mean consumers will encounter a range of new cyber safety challenges. Consumer demands and behaviors are rapidly changing and driving more activities online, from shopping, socializing, working, banking, to other activities in healthcare, entertainment and so much more. Almost every aspect of a person' s life has a digital component. Unfortunately, many of those activities are left unprotected, and attackers are exploiting this larger opportunity and the inherent security and privacy vulnerabilities. Cybercriminals have not only expanded their reach, but the sophistication of digital threats and attacks are becoming increasingly more realistic and believable. The advancement of AI and large language model (LLM) technology is a key driver of this increased risk. Cybercrime, and the ways in which cybercriminals target consumers, continue to evolve along with behaviors and technology. Cybercrime encompasses any crime committed with devices over the internet and includes crimes where (i) malicious software or unauthorized access is detected on a device, network or online account (such as email, social media, online banking, digital assets, online retail, gaming, online entertainment, etc.), and unauthorized access or connection to cloud service accounts; (ii) an individual is digitally victimized through a data breach, cyber theft, cyber extortion, or fraud (stolen personally identifiable information, identity theft, etc.); (iii) online stalking, bullying, or harassment is inflicted; or (iv) attacks related to privacy or disinformation (such as online tracking protection, identity impersonation, disinformation on social media, deepfakes, unsecured WiFi, EvilTwin attacks, etc.). Competitive Landscape We operate in a highly competitive and dynamic environment. We face global competition from a broad range of companies, including software vendors focusing on cyber safety solutions, operating system providers such as Apple, Google and Microsoft, and ' pure play' companies that currently specialize in one or a few particular segments of the market (many of which are expanding their product portfolios into different segments). We believe the competitive factors in our market include innovation, access to a breadth of identity and consumer transaction data, broad and effective service offerings, brand recognition, technology, effective and cost- efficient customer acquisition, strong retention rate, customer satisfaction, price, convenience of purchase, ease of use, frequency of upgrades and updates and quality and reliable customer service. Our competitors may vary by offering, geography, business model and channel. Our principal competitors are set forth below: • Security: Our principal competitors in this segment include Apple, Bitdefender, ESET, F- Secure, Google, Kaspersky, Malwarebytes, McAfee, Microsoft, Trend Micro, and Webroot. • Identity Protection: Our principal competitors in this segment include credit bureaus such as Equifax, Experian and TransUnion, as well as certain credit monitoring and identity theft protection solutions from others such as Allstate, Aura, Generali (Iris), Intuit (Credit Karma) and Microsoft. • Online Privacy: Our principal competitors in this segment include Apple, Aura, Brave, DuckDuckGo, IPVanish, Kape, Mozilla and Nord Security. • Other Competitors: In addition to competition from independent software vendors such as Bitdefender , Kaspersky, McAfee and Trend Micro, and from OS providers such as Apple, Google and Microsoft, we also face competition from other companies that currently focus on one or a few cyber safety or adjacent segments but are developing additional competing products and expanding their portfolios into

new segments, such as ‘ pure play’ companies including but not limited to, 1Password, Bark, Dashlane, LastPass, Life360, Proton, and Truecaller, internet service providers, big tech platform providers, insurance companies and financial service organizations. We believe we compete favorably with our competitors on the strength of our technology, people, product offerings and presence in all of the current key cyber safety categories. However, some of our competitors have greater financial, technical, marketing, distribution or other resources than we do, including in new cyber safety and digital life segments we may enter, which consequently affords them competitive advantages. As a result, they may be able to devote greater resources to develop, promote and sell their offerings; deliver competitive offerings at lower prices or for free; and introduce new solutions and respond to market developments and customer requirements and preferences more quickly or cost effectively than we can. In addition, for individual solutions or features, smaller, well- funded competitors may be able to innovate and adapt more nimbly to the dynamic nature of the market and shifting consumer needs. For more information on the risks associated with our competitors, please see “ Risk Factors ” – Risks Related to Our Business Strategy and Industry – “ We operate in a highly competitive and dynamic environment, and if we are unable to compete effectively, we could experience a loss in market share and a reduction in revenue ” and “ We may need to change our pricing models to compete successfully, ” in Item 1A included in this Annual Report on Form 10- K. Human Capital Management At Gen, our mission is to build a comprehensive and easy- to- use integrated portfolio that prevents, detects and responds to cyber threats and cybercrimes in today’ s digital world. Our success in helping achieve this mission depends, in large part, on the success of our employees. • General Employee Demographics: As of March 28, 2025, we employed just under 3, 500 team members in over 20 countries worldwide. With dual headquarters in Tempe, Arizona, and in Prague, Czech Republic, we have over 1, 000 active employees located in the U. S. and nearly 900 active employees in the Czech Republic. None of our U. S. employees are represented by a labor union or covered by a collective bargaining agreement. • Employee Development and Training: Our people programs are designed to provide our team members with support, resources, and opportunities they need to grow, learn and thrive in their careers. We continued to focus on learning and development in fiscal 2025, investing further in digital learning via our Learn @ Gen program for all employees. Leveraging an extensive breadth of content and learning opportunities, this umbrella of offerings includes LinkedIn Learning catalog, Gen Mentorship, Academics and leadership trainings. • Employee Engagement: We value our people and are committed to creating a positive and fulfilling experience for everyone. Feedback from our employees is critical, and we have developed an ongoing dialogue with our teams via our Engage pulse survey on a targeted topic that drives actions and improvements. • Benefits, Health and Wellness: At Gen, we value our people and are committed to creating a positive and fulfilling experience for everyone through the programs and benefits we offer. Our employee value proposition, Life @ Gen is centered on choice, flexibility and growth and encompasses the many elements of our employee experience. Our commitment to overall health and wellness is centered around having an integrated and equitable wellness program that supports body, mind and financial health. • Human Capital Governance: We partner closely with our Board of Directors and the Compensation and Leadership Development Committee on executive compensation, our broader reward strategies and objectives related to talent management, talent acquisition, leadership development, retention and succession, and employee engagement. Intellectual Property Our intellectual property (IP) is an important and vital asset that enables us to develop, market, and sell our software products and services and enhance our competitive position. We are a leader among consumer cyber safety solutions in pursuing patents and currently have a portfolio of over 1, 000 U. S. and international patents issued with many additional patents pending. We protect our intellectual property rights and investments in a variety of ways to safeguard our technologies and our long- term success. Our IP portfolio is spread across different entities and in multiple countries. As we continue to expand our international operations, we have developed a strategy to ensure global distribution of our IP aligns with our long- term strategic objectives, business model, and goals. We work actively in the U. S. and internationally to ensure the enforcement of copyright, trademark, trade secret and other protections that apply to our software products and services. The term of the patents we hold is, on average, in excess of ten years. From time to time, we enter into cross- license agreements with other technology companies covering broad groups of patents; we have an additional portfolio of over 2, 000 U. S. and international patents cross- licensed to us as part of our arrangement with Broadcom as a result of the asset sale of our former Enterprise Security business. We also use software from third parties in our business and generally must rely on those third parties to protect the licensed rights. This can include open source software, which is subject to limited proprietary rights. While it may be necessary in the future to seek or renew licenses relating to various aspects of our products, services, and business methods, we believe, based upon past experience and industry practice, such licenses generally can be obtained on commercially reasonable terms. The ability to maintain and protect our intellectual property rights is important to our success, but we believe our business is not materially dependent on any individual patent, copyright, trademark, trade secret, license, or other intellectual property right. However, circumstances outside our control could pose a threat to our intellectual property rights. Effective intellectual property protection may not be available, and the efforts we have taken to protect our proprietary rights may not be sufficient or effective. Any significant impairment of our intellectual property rights could harm our business or our ability to compete. In addition, protecting our intellectual property rights is costly and time consuming. Any unauthorized disclosure or use of our intellectual property could make it more expensive to do business and harm our operating results. In addition, a large number of patents, copyrights and trademarks are owned by other companies in the technology industry. Those companies may request license agreements, threaten litigation, or file suit against us based on allegations of infringement or other violations of intellectual property rights. For more information on the risks associated with our intellectual property, please see “ Risk Factors ” in Item 1A included in this Annual Report on Form 10- K. Governmental Regulation We collect, use, store or disclose an

increasingly high volume, and variety of personal information , including **from employees and customers, in connection with the operation of our business, particularly, in relation to our identity and information protection offerings, which rely on large data repositories of personal information and consumer transactions. The personal information we process is subject to an increasing number of federal, state, local and foreign laws regarding privacy and data security. For information on the risks associated with complying with privacy and data security laws, please see " Risk Factors " in Item 1A included in this Annual Report on Form 10- K. Available Information Our internet homepage is located at GenDigital. com. We make available our annual reports on Form 10- K, quarterly reports on Form 10- Q, current reports on Form 8- K, and amendments to those reports as soon as reasonably practicable after we electronically file such material with the SEC on our investor relations website located at Investor. GenDigital. com. We also use our website as a tool to disclose important information about the company and comply with our disclosure obligations under Regulation Fair Disclosure. The information contained, or referred to, on our website, including in any reports that are posted on our website, is not part of this annual report unless expressly noted. The SEC maintains a website that contains reports, proxy and information statements, and other information regarding our filings at http: / / www. sec. gov. Item 1A. Risk Factors A description of the risk factors associated with our business is set forth below and in " Management' s Discussion and Analysis of Financial Condition and Results of Operations, Legal Proceedings, and Quantitative and Qualitative Disclosures About Market Risk. " The list is not exhaustive, and you should carefully consider these risks and uncertainties before investing in our common stock. RISKS RELATED TO OUR BUSINESS STRATEGY AND INDUSTRY If we are unable to develop new and enhanced solutions, or if we are unable to continually improve the performance, features, and reliability of our existing solutions, our business and operating results could be adversely affected. Our future success depends on our ability to effectively respond to evolving threats to consumers, as well as competitive technological developments and industry changes, by developing or introducing new and enhanced solutions and products on a timely basis. In the past, we have incurred, and will continue to incur, significant research and development expenses as we focus on organic growth through internal innovation. We believe that we must continue to dedicate significant resources to our research and development efforts to deliver innovative market competitive products and avoid being reliant on third- party technology and products. If we do not achieve the benefits anticipated from these research and development investments, or if the achievement of these benefits is delayed, our operating results may be adversely affected. We must continually address the challenges of dynamic and accelerating market trends and competitive developments. Customers may require features and capabilities that our current solutions do not have. Our failure to develop new solutions and improve our existing solutions to satisfy customer preferences and effectively compete with other market offerings in a timely and cost- effective manner may harm our ability to retain our customers and attract new customers. For example, the process of developing and integrating new technologies, including generative artificial intelligence (" Gen AI ") and machine learning models, is complex, time- consuming and may cause errors or inadequacies that are not easily detectable. As we integrate more Gen AI technology into our platform to improve the experience of our users and meet the demands of our customers, it may result in unintentional or unexpected outputs that are incorrect or biased and cause customer dissatisfaction or subject us to lawsuits, reputational harm and increased regulatory scrutiny. The development and introduction of new solutions involve significant commitments of time and resources and are subject to risks and challenges including but not limited to: • Lengthy development cycles; • Evolving industry and regulatory standards and technological developments, including AI and machine learning, by our competitors and customers; • Rapidly changing customer preferences and accurately anticipating technological trends or needs; • Evolving platforms, operating systems, and hardware products, such as mobile devices; • Product and service interoperability challenges with customer' s technology and third- party vendors; • The integration of products and solutions from acquired companies; • Availability of engineering and technical talent; • Entering new or unproven market segments; • New and evolving regulation; and • Executing new product and service strategies. In addition, third parties, including, but not limited to,** operating systems and internet browser companies, have in the past and may in the future limit the interoperability of our solutions with their own products and services, in some cases to promote their own offerings or those of our competitors. Any such actions by third parties could delay the development of our solutions **and products** or our solutions **and products** may be unable to operate effectively. This could also result in decreased demand for our solutions **and products** , decreased revenue, harm to our reputation, and adversely affect our business, financial condition, results of operations, and cash flows. If we are not successful in managing these risks and challenges, or if our new or improved solutions **or products** are not technologically competitive or do not achieve market acceptance, our business and operating results could be adversely affected. We operate in ~~a highly competitive and dynamic environment, and if we are unable to compete effectively, we could experience a loss in market share and a reduction in revenue. We operate in~~ intensely competitive and dynamic markets that experience frequent and rapid technological developments, changes in industry and regulatory standards, evolving market trends, changes in customer requirements and preferences, and frequent new product introductions and improvements. If we are unable to anticipate or react to these continually evolving conditions, we could experience a loss of market share and a reduction in our revenues, which could materially and adversely affect our business and financial results. To compete successfully, we must maintain an innovative research and development effort to develop new solutions and **products and** enhance our existing solutions **and products** , and effectively adapt to changes in the **technology, financial** technology, privacy and data protection standards or trends. We face competition from a broad range of companies, including software vendors focusing on cyber safety solutions such as Bitdefender, Kaspersky, McAfee and Trend Micro, operating system providers such as Apple, Google and Microsoft, and companies such as Nord, Life360, LastPass and others that currently specialize in one or a few particular segments of the market and many of which are expanding their product portfolios into different segments. ~~Many of these competitors offer solutions or~~

~~are currently developing solutions that directly compete with some or all of our offerings.~~ We also face growing competition from other technology companies, as well as from companies in the identity threat protection space such as credit bureaus. Further, many of our competitors are increasingly developing and incorporating into their products data protection software and other competing cyber safety products **,** such as antivirus protection or VPN, often free of charge, that compete with our offerings. Our competitive position could be adversely affected by the functionality incorporated into these products rendering our existing solutions obsolete and therefore causing us to fail to meet customer expectations. **For our MoneyLion business, we face competition from a broad range of companies across our business lines, including traditional banks and credit unions; new entrants obtaining banking licenses; non- bank digital providers offering banking- related services; specialty finance and other non- bank digital providers offering consumer lending- related or earned wage access products; digital wealth management platforms such as robo- advisors offering consumer investment services and other brokerage- related services; and digital financial platform, embedded finance and marketplace competitors, which aggregate and connect consumers to financial product and service offerings. We also compete with advertising agencies and other service providers to attract marketing budget spending from our Enterprise clients. We expect our competition to continue to increase, as there are generally no substantial barriers to entry to the markets we serve. Some of our current and potential competitors have longer operating histories, particularly with respect to financial services products similar to ours, significantly greater resources and a larger customer base than we do. This allows them, among other things, to potentially offer more competitive pricing or other terms or features, a broader range of financial or other products or a more specialized set of specific products or services, as well as respond more quickly than we can to new or emerging technologies and changes in consumer preferences.** In addition, the introduction of new products or services by **existing or future** competitors, and / or market acceptance of products or services based on emerging or alternative technologies, could make it easier for other products or services to compete with our solutions ~~. We have seen~~ and **reduce** ~~anticipate additional competition as new participants enter the cyber safety market and as~~ our ~~current competitors seek to increase their~~ market share **in** ~~and expand their~~ -- **the future** ~~existing offerings. Some of our competitors have greater financial, technical, marketing, or other resources than we do, including in new cyber safety and digital life segments. Consequently, those competitors may influence customers to purchase their products instead of ours through investing more in internal innovation than we can and through their unique access to customer engagement points~~ . Further consolidation among our competitors and within our industry or, in addition to other changes in the competitive environment, such as greater vertical integration from key computing and operating system suppliers could result in larger competitors that compete more frequently with us. ~~In~~ **Specifically, in** addition to competing with ~~these~~ **cyber safety** vendors directly for sales to end- users of our solutions, we compete with them for the opportunity to have our solutions bundled with the offerings of our strategic partners, such as computer hardware OEMs, internet service providers, operating systems and telecom service providers. Our competitors could gain market share from us if any of these strategic partners replace our solutions with those of our competitors or with their own solutions **or** ~~. Similarly, they could gain market share from us if these partners~~ promote our competitors' solutions or their own solutions more frequently or more favorably than our solutions. In addition, software vendors who have bundled our solutions with theirs may choose to bundle their solutions with their own or other vendors' solutions or may limit our access to standard interfaces and inhibit our ability to develop solutions for their platform. Further product development by these vendors could cause our solutions to become redundant, which could significantly impact our sales and operating results. We cannot be sure that we will accurately predict how the markets in which we compete or intend to compete will evolve. Failure on our part to anticipate changes in our markets and to develop solutions and enhancements that meet the demands of those markets or to effectively compete against our competitors will significantly impair our business, financial condition, results of operations, and cash flows. ~~Issues in the development and deployment of AI may result in reputational harm and legal liability and could adversely affect our results of operations.~~ We have incorporated, and are continuing to develop and deploy, AI **, including Gen AI,** into many of our products, solutions and services. AI presents challenges and risks that could affect our products, solutions and services, and therefore our business. For example, AI algorithms may **be flawed, insufficient, of poor quality, reflect unwanted forms of bias, or contain other errors or inadequacies, any of which may not be easily detectable; AI has been known to produce false or " hallucinatory " inferences or outputs; AI can present ethical issues and may subject us to new or heightened legal, regulatory, ethical, or other challenges, including issues relating to discrimination, intellectual property infringement or misappropriation, violation of rights of publicity, inability to assert ownership of inventions and works of authorship, loss of trade secrets, defamation, data privacy and cybersecurity; and inappropriate or controversial data practices by developers and end- users, or other factors adversely affecting public opinion of AI, could impair the acceptance of AI solutions, including those incorporated in our products and services. If the AI solutions that we create or use are deficient, inaccurate or controversial, we could incur operational inefficiencies, competitive harm, legal liability, brand or reputational harm, or other adverse impacts on our business and financial results. In addition, if we do not** have **sufficient rights to use the data or other material or content on which our AI tools rely, we also may incur liability through the violation of applicable** ~~flaws~~ -- **laws** ~~,~~ and **regulations, third- party intellectual property, privacy or other rights, or contracts to which we are a party. The use or adoption of AI technologies in our products may also result in exposure to claims by third parties of copyright infringement or other intellectual property misappropriation, which may require us to pay compensation or license fees to third parties. For example, the large** datasets used to train **Gen AI technologies** ~~models may be insufficient~~ or **output generated by Gen AI technologies may** contain **materials that may** ~~biased information. These potential issues could~~ subject us to **third- party claims of intellectual property infringement or violations of rights of publicity. This risk is exacerbated with respect to our use of third- party Gen AI technologies, as it can be very difficult, if not impossible, to validate the processes used by third- party Gen AI technology providers in their collection and use of training data or the algorithm to produce outputs. In addition,**

regulation of Gen AI is rapidly evolving worldwide as legislators and regulators are increasingly focused on these powerful emerging technologies. The technologies underlying Gen AI and its uses are currently subject to a variety of laws and regulations, including intellectual property, privacy, data protection and information security, consumer protection, competition, and equal opportunity laws, and are expected to be subject to increased regulation and new laws or new applications of existing laws and regulations. Gen AI is the subject of ongoing review by various U. S. governmental and regulatory ~~risk~~ **agencies , and various U. S. states and other foreign jurisdictions are applying, or are considering applying, their platform moderation, cybersecurity, and data protection laws and regulations to Gen AI or are considering general** legal ~~liability~~ **frameworks for Gen AI. For example, the EU AI Act, which came into force on August 1, 2024, will generally become fully applicable after a two- year transitional period, with certain obligations taking effect at an earlier or later time. The EU AI Act introduces various requirements for AI systems and models placed on the market or put into service in the EU** , including ~~under new~~ **specific transparency and other requirements for general** ~~proposed -- purpose legislation regulating~~ AI ~~in jurisdictions such as~~ **systems and the models on which** ~~the~~ **they** ~~EU and~~ **are based. In addition, several U. S. states are considering enacting or have already enacted** regulations ~~being considered~~ **concerning the use of AI technologies. At the federal and state level, there have been various proposals (and** in **some cases laws enacted) addressing " deepfakes " and** other ~~jurisdictions~~ **AI- generated synthetic media. Furthermore** , ~~and~~ **because AI technology itself is highly complex** ~~brand --~~ **and rapidly developing, it is not possible to predict all of the legal, operational** or ~~reputational harm~~ **technological risks that may arise relating to the use of AI** . The rapid evolution of AI, including potential government regulation of AI, requires us to invest significant resources to develop, test, and maintain AI in our products and services in a manner that meets evolving requirements and expectations ~~. The rules~~ and **we** ~~regulations adopted by policymakers over time~~ may **need** ~~require us~~ to ~~make changes~~ **expend resources** to **adjust** our ~~business practices~~ **offerings in certain jurisdictions if the legal frameworks are inconsistent across jurisdictions** . Developing, testing, and deploying AI systems may also increase the cost profile of our offerings due to the nature of the computing costs involved in such systems. ~~The intellectual property ownership and license rights surrounding AI technologies, as well as data protection laws related to the use and development of AI, are currently not fully addressed by courts or regulators. The use or adoption of AI technologies in our products may result in exposure to claims by third parties of copyright infringement or other intellectual property misappropriation, which may require us to pay compensation or license fees to third parties. The evolving legal, regulatory, and compliance framework for AI technologies may also impact our ability to protect our own data and intellectual property against infringing use. Our acquisitions and divestitures create special risks and challenges that could adversely affect our financial results.~~ As part of our business strategy, we may acquire or divest businesses or assets. For example, in 2019, we completed the sale of certain of our enterprise security assets to Broadcom Inc. (the Broadcom sale), in January 2021, we completed the acquisition of Avira, ~~and~~ in September 2022, we completed the acquisition of Avast **, and in April 2025, we completed the acquisition of MoneyLion** . Our acquisition and divestiture activities have and may continue to involve a number of risks and challenges, including: • Complexity, time and costs associated with managing these transactions, including the integration of acquired and the winding down of divested business operations, workforce, products, **services,** IT systems and technologies **; • Challenges in maintaining uniform standards, controls, procedures and policies within the combined organization** ; • Challenges in retaining the customers of acquired businesses, providing the same level of service to existing customers with reduced resources, or retaining the third- party relationships, including with suppliers, service providers, and vendors, among others; • Diversion of management time and attention; • Loss or termination of employees, including costs and potential institutional knowledge loss associated with the termination or replacement of those employees; • Assumption of liabilities of the acquired and divested business or assets, including pending or future litigation, investigations or claims related to the acquired business or assets; • Addition of acquisition- related debt; • Difficulty entering into or expanding in new markets or geographies; • Increased or unexpected costs and working capital requirements; • Dilution of stock ownership of existing stockholders; • Ongoing contractual obligations and unanticipated delays or failure to meet contractual obligations **; • Regulatory risks, including remaining in good standing with existing regulatory bodies or receiving any necessary approvals, as well as being subject to new regulators with oversight over an acquired business** ; • Substantial accounting charges for acquisition- related costs, asset impairments, amortization of intangible assets and higher levels of stock- based compensation expense; and • Difficulty in realizing potential benefits, including cost savings and operational efficiencies, synergies and growth prospects from integrating acquired businesses. **We may not be able to identify appropriate business opportunities that benefit our business strategy or otherwise satisfy our criteria to undertake such opportunities. Even if we do identify potential strategic transactions, we may not be successful in negotiating favorable terms in a timely manner or at all or in consummating the transaction, and even if we do consummate such a transaction, it may not generate sufficient revenue to offset the associated costs, may not otherwise result in the intended benefits or may result in unexpected difficulties and risks.** Macroeconomic factors, such as **fluctuating tariffs, trade wars.** high inflation, high interest rates, and volatility in foreign currency exchange rates and capital markets could negatively influence our future acquisition opportunities. Moreover, to be successful, large complex acquisitions depend on large- scale product, technology, and sales force integrations that are difficult to complete on a timely basis or at all and may be more susceptible to the special risks and challenges described above. Any of the foregoing, and other factors, could harm our ability to achieve anticipated levels of profitability or other financial benefits from our acquired or divested businesses, product lines or assets or to realize other anticipated benefits of divestitures or acquisitions. ~~Our revenue and operating results depend significantly on our ability to retain our existing customers and expand sales to them, convert existing non- paying customers to paying customers and add new customers. We generally sell our solutions to our customers on a monthly or annual subscription basis.~~ It is important to our **cyber and financial technology** ~~business~~ **businesses** that we retain existing customers and that our customers expand their use of our solutions **and products** over time **. If our efforts to sell additional functionality, products and services to our**

customers and clients are not successful, our business and growth prospects would suffer . Customers may choose not to renew their membership with us at any time **and may stop utilizing our products that generate us revenue from transaction, interchange or transfer fees, among others** . **For our solutions sold to customers on a monthly or annual subscription basis,** ~~Renewing~~ **renewing** customers may require additional incentives to renew, may not renew for the same contract period, or may change their subscriptions. We therefore may be unable to retain our existing customers on the same or more profitable terms, if at all. In addition, we may not be able to accurately predict or anticipate future trends in customer retention or effectively respond to such trends. Our customer retention rates may decline or fluctuate due to a variety of factors, including the following: • Our customers' levels of satisfaction or dissatisfaction with our solutions and the value they place on our solutions; • The quality, breadth, and prices of our solutions, including solutions offered in emerging markets; • Our general reputation and events impacting that reputation; • The services and related pricing offered by our competitors; including increasing the availability and efficacy of free solutions **; • Increases in costs we incur and may pass on to our customers in order to offer our products or services** ; • Disruption by new services or changes in law or regulations that impact the need for or efficacy of our products and services; • Changes in auto- renewal and other consumer protection regulations; • Our customers' dissatisfaction with our efforts to market additional products and services; • Our customer service and responsiveness to the needs of our customers; • Changes in our target customers' spending levels as a result of general economic conditions, inflationary pressures or other factors; and • The quality and efficacy of our third- party partners who assist us in renewing customers' subscriptions. Declining customer retention rates could cause our revenue to grow more slowly than expected or decline, and our operating results, gross margins and business will be harmed. In addition, our ability to generate revenue and maintain or improve our results of operations partly depends on our ability to cross- sell our solutions to our existing customers and to convert existing non- paying customers to paying customers and add new customers. We may not be successful in cross - selling our solutions because our customers may find our additional solutions unnecessary or unattractive. Our failure to sell additional solutions to our existing customers, failure to convert existing non- paying customers to paying customers or add new customers could adversely affect our ability to grow our business. An important part of our growth strategy involves continued investment in direct marketing efforts, indirect partner distribution channels **, expanding enterprise partner relationships** , freemium channels, our sales force, and infrastructure to add new customers. The number and rate at which new customers purchase our products and services depends on a number of factors, including those outside of our control, such as customers' perceived need for our solutions **and products** , competition, general economic conditions, market transitions, product obsolescence, technological change, public awareness of security threats to IT systems, macroeconomic conditions, and other factors. New customers, if any, may subscribe or renew their subscriptions **, or utilize our products and solutions,** at lower rates than we have experienced in the past, introducing uncertainty about their economic attractiveness and potentially impacting our financial results. Additionally, there are inherent challenges in measuring the usage of our products and solutions across our brands, platforms, regions, and internal systems, and therefore, calculation methodologies for direct customer counts may differ, which may impact our ability to measure the addition of new customers **and our understanding of certain details of our business** . The methodologies used to measure these metrics require judgment and are also susceptible to algorithms or other technical errors ~~. We continually seek to improve our estimates of our user base, and these estimates are subject to change due to improvements or revisions to our methodology~~ . From time to time, we review our metrics and may discover inaccuracies or make adjustments to improve their accuracy, which can result in adjustments to our historical metrics. Our ability to recalculate our historical metrics may be impacted by data limitations or other factors that require us to apply different methodologies for such adjustments. **If investors do not perceive our operating metrics to be accurate, or if we discover material inaccuracies with respect to these figures, our reputation may be significantly harmed, and our results of operations and financial condition could be adversely affected.** We may need to change our pricing models to compete successfully. The intense competition we face, in addition to general and economic business conditions (including **rising government debt levels, potential government policy shifts, changing U. S. consumer spending patterns,** economic volatility, bank failures **, fluctuating tariff rates, trade wars** , and high inflation and interest rates, among other things), may put pressure on us to change our pricing practices **. In particular, the ongoing global conflicts could amplify disruptions to the financial and credit markets, increase risks of an information security or operational technology incident, cause cost fluctuations to us or third parties upon which we rely and increase costs to ensure compliance with global and local laws and regulations** . If our competitors offer deep discounts on certain solutions, provide offerings, or offer free introductory products that compete with ours, we may **experience pricing pressure and may be unable to retain current customers and clients or attract new customers and clients at consistent prices within our operating budget. Or we may** need to lower our prices or offer similar free introductory products to compete successfully. Similarly, if external factors, such as economic conditions, market trends, or business combinations require us to raise our prices, our ability to acquire new customers and retain existing customers may be diminished. Any such changes may reduce revenue and margins and could adversely affect our financial results. Additionally, changes in the macroeconomic environment have previously and may continue to affect our business. Our solutions are discretionary purchases, and customers may reduce or eliminate their discretionary spending on our solutions during a difficult macroeconomic environment. We may experience a material increase in cancellations by customers or a material reduction in our retention rate in the future, especially in the event of a prolonged recession or a worsening of current conditions as a result of **trade wars, fluctuating tariff rates,** inflation, changes in interest rates, **government shutdowns, political developments and unrest** or other macroeconomic events. We may have to lower our prices or make other changes to our pricing model to address these dynamics, any of which could adversely affect our business and financial results. Many of Avira' s and Avast' s users are freemium subscribers, meaning they do not pay for its basic services. Much of our anticipated growth in connection with the Avira and Avast acquisitions are attributable to attracting and converting Avira' s and Avast' s freemium users to a paid subscription option. Numerous factors, however, have previously and may continue to

impede our ability to attract and retain free users, convert these users into paying customers and retain them as paying customers. ~~If we fail to manage our sales and distribution channels effectively, or if our partners choose not to market and sell our solutions to their customers, our operating results could be adversely affected.~~ A portion of our revenues is derived from sales through indirect channels, including, but not limited to, distributors that sell our products to end- users and other resellers, and partners that incorporate our products into, or bundle our products with, their products. These channels involve risks, including: • Our resellers, distributors and telecom service providers are generally not subject to minimum sales requirements or any obligation to market our solutions to their customers; • Our reseller and distributor agreements are generally nonexclusive and may be terminated at any time without cause and our partners may terminate or renegotiate their arrangements with us and new terms may be less favorable due to competitive conditions in our markets and other factors; • Our resellers ~~,~~ **and** distributors ~~and OEMs~~ may encounter issues or have violations of applicable law or regulatory requirements or otherwise cause damage to our reputation through their actions; • Our resellers and distributors frequently market and distribute competing solutions and may, from time to time, place greater emphasis on the sale of competing solutions due to pricing, promotions and other terms offered by our competitors; • Any consolidation of electronics retailers can increase their negotiating power with respect to software providers such as us and any decline in the number of physical retailers could decrease the channels of distribution for us; • The consolidation of online sales through a small number of larger channels has been increasing, which could reduce the channels available for online distribution of our solutions; and • Sales through our partners are subject to changes in general economic conditions, strategic direction, competitive risks, and other issues that could result in fewer sales, or cause our partners to suffer financial difficulty which could delay payments to us, affecting our operating results. If we fail to manage our sales and distribution channels successfully, these channels may conflict with one another or otherwise fail to perform as we anticipate, which could reduce our sales and increase our expenses as well as weaken our competitive position. ~~Changes~~ **In our MoneyLion business, our success also depends** in ~~industry structure~~ **part on the delivery of qualified consumer lead inquiries** and **conversions to completed transactions for various financial products to Product Partners. However, the failure of our Enterprise platform to effectively connect and match consumers from our Channel Partners with product offerings from our Product Partners in a manner that results in converted customers and increased revenue for such Product Partners could cause Product Partners to cease spending** ~~market~~ **marketing funds on our Enterprise platform, which could have a material adverse impact on our ability to maintain or increase our Enterprise revenue. Any factors that limit the amount that our Product Partners are willing to, and do, spend on marketing or advertising with us could have a material adverse effect on our business, financial condition, results of operations and cash flows. Additionally, during challenging macroeconomic** conditions ~~have and~~ **, our Product Partners** may **tighten underwriting standards for** ~~continue to lead to charges related to discontinuance of~~ certain of ~~our~~ **their** products **, which would result in fewer opportunities** ~~or~~ **for us to generate revenue from matching consumers from our Channel Partners with them. The success of our** ~~businesses -- business~~ and ~~asset impairments~~ **our ability to engage and retain customers in our platform are dependent in part on our ability to produce or acquire popular content, which in turn depends on our ability to retain content creators and rights to content for our platform. We may in the future incur increasing revenue-sharing costs to compensate content creators for producing original content. Any changes in these relationships or loss of these partners or vendors, any failure of them to perform their obligations in a timely manner or at all or if they were to cease to provide such functions for any reason, could degrade the functionality of our platform, materially and adversely affect usage of our products and services, impose additional costs or requirements or disadvantage us compared to our competitors. We also rely on relationships with third- party partners to obtain and maintain customers, and our ability to acquire new customers could be materially harmed if we are unable to enter into or maintain these relationships on terms that are commercially reasonable to us, or at all. In the event that such a third party for any reason fails to comply with legal or regulatory requirements or otherwise to perform its functions properly, our ability to conduct our business and perform other operational functions for which we currently rely on such third party will suffer, and our business, financial condition, results of operations and cash flows may be negatively impacted** . In response to changes in industry structure and market conditions, we have been and may continue to be required to strategically reallocate our resources and consider restructuring, disposing of, or otherwise exiting certain businesses. Any decision to limit investment in or dispose of or otherwise exit businesses has and may continue to result in the recording of special charges, such as technology- related write-offs, workforce reduction costs, charges relating to consolidation of excess facilities, or claims from third parties who were resellers or users of discontinued products. Our estimates with respect to the useful life or ultimate recoverability of our carrying basis of assets, including purchased intangible assets, could change as a result of such assessments and decisions. Our loss contingencies have and may continue to include liabilities for contracts that we cannot cancel, reschedule or adjust with suppliers. Further, our estimates relating to the liabilities for excess facilities are affected by changes in real estate market conditions. Additionally, we are required to evaluate goodwill impairment on an annual basis and between annual evaluations in certain circumstances. Goodwill impairment evaluations have previously and may result in a charge to earnings. RISKS RELATED TO OUR OPERATIONS **We** ~~Our international operations involve risks that could increase our expenses, adversely affect our operating results and require increased time and attention of our management. Following the acquisition of Avast, we~~ derive a significant portion of our revenues from customers located outside of the United States, and we have substantial operations outside of the United States, including engineering, finance, sales and customer support. Our international operations are subject to risks in addition to those faced by our domestic operations, including: • Difficulties staffing, managing, and coordinating the activities of our geographically dispersed and culturally diverse operations; • Potential loss of proprietary information due to misappropriation or laws that may be less protective of our intellectual property rights than U. S. laws or that may not be adequately enforced; • Requirements of foreign laws and other governmental controls, including tariffs, trade barriers and labor restrictions, and related laws that reduce the flexibility of our business operations; • Fluctuations in currency

exchange rates, economic instability and inflationary conditions could make our solutions more expensive or could increase our costs of doing business in certain countries; • ~~Potential changes~~ **Changes** in trade relations arising from policy initiatives or other political factors; • Regulations or restrictions on the use, import or export of encryption technologies that could delay or prevent the acceptance and use of encryption products and public networks for secure communications **; • Regulations or restrictions regarding the collection, processing, sharing, transfer, portability, security and storage of consumer data (including personal information), including privacy and data protection laws** ; • Local business and cultural factors that differ from our normal standards and practices, including business practices that we are prohibited from engaging in by the Foreign Corrupt Practices Act and other anti- corruption laws and regulations; • Central bank and other restrictions on our ability to repatriate cash from our international subsidiaries or to exchange cash in international subsidiaries into cash available for use in the United States; • Limitations on future growth or inability to maintain current levels of revenues from international sales if we do not invest sufficiently in our international operations; • Difficulties in staffing, managing and operating our international operations; • Costs and delays associated with developing software and providing support in multiple languages; • Political, social or economic unrest, war, terrorism, regional natural disasters, or export controls and trade restrictions, particularly in areas in which we have facilities **and in areas where our engineering and technical development teams are based** ; and • Multiple and possibly overlapping tax regimes. The expansion of our existing international operations and entry into additional international markets has required and will continue to require significant management attention and financial resources. These increased costs may increase our cost of acquiring international customers, which may delay our ability to achieve profitability or reduce our profitability in the future. We also have and may continue to face pressure to lower our prices in order to compete in emerging markets, which has previously and could in the future adversely affect revenue derived from our international operations. It is not possible to predict the broader consequences of **existing** geopolitical conflicts ~~, such as the Russia- Ukraine conflict, and the numerous conflicts in the Middle East,~~ and other conflicts that may arise in the future, which could include geopolitical instability and uncertainty; adverse impacts on global and regional economic conditions and financial markets, including significant volatility in credit, capital, and currency markets; reduced economic activity; changes in laws and regulations affecting our business, including further sanctions or counter- sanctions which may be enacted; and increased cybersecurity threats and concerns. The ultimate extent to which such conflicts may negatively impact our business, financial condition and results of operations will depend on future developments, which are highly uncertain, difficult to predict and subject to change ~~. Our future success depends on our ability to attract and retain personnel in a competitive marketplace~~ . Our future success depends upon our ability to recruit and retain key management, technical (including cyber security and AI experts), sales, marketing, e- commerce, finance and other personnel. Our officers and other key personnel are " at will " employees and we generally do not have employment or non- compete agreements with our employees. Competition is significant for people with the specific skills that we require, including in the areas of AI and machine learning, and especially in the locations where we have a substantial presence and need for such personnel. In order to attract and retain personnel in a competitive marketplace, we must provide competitive pay packages, including cash and equity- based compensation. Additionally, changes in immigration laws could impair our ability to attract and retain highly qualified employees. If we fail to attract, retain and motivate new or existing personnel, our business, results of operations and future growth prospects could suffer. Volatility in our stock price may from time to time adversely affect our ability to recruit or retain employees. In addition, we may not have an adequate number of shares reserved under our equity compensation plans, forcing us to reduce awards of equity- based compensation, which could impair our efforts to attract, retain and motivate necessary personnel. If we are unable to hire and retain qualified employees, or conversely, if we fail to manage employee performance or reduce staffing levels when required by market conditions, our business and operating results could be adversely affected. Effective succession planning is also important to our long- term success. Failure to ensure effective transfer of knowledge and smooth transitions involving key employees could hinder our strategic planning and execution. From time to time, key personnel leave our company and the frequency and number of such departures have widely varied and have, in the past, resulted **, and may in the future result** in significant changes to our executive leadership team. The loss of any key employee could result in significant disruptions to our operations, including adversely affecting the timeliness of product releases, the successful implementation and completion of company initiatives, our internal control over financial reporting and our results of operations. In addition, hiring, training and successfully integrating replacement personnel can be time consuming and expensive, may cause additional disruptions to our operations and may be unsuccessful, which could negatively impact future financial results. Our ~~solutions, systems, websites~~ **decisions to provide many of our products** and **services to customers are based partly on information that** ~~the~~ **they provide to us or authorize us to receive from third party sources. To the extent that these customers or third parties provide information to us in a manner that we are unable to verify, our decisioning process may not accurately reflect the associated risk. In addition,** data **provided by third- party sources, including consumer reporting agencies, is a component of our credit decisions and this data may contain inaccuracies. This may result in the inability to either approve otherwise qualified applicants or rejected otherwise unqualified applicants through our platform or accurately analyze credit data, which may adversely impact our business and negatively impact our reputation. In addition, there is risk of fraudulent activity associated with our business, including as a result of the service providers and other third parties who handle customer information** on **our behalf. We use identity and fraud prevention tools to analyze data provided by external databases to authenticate the identity of each applicant that signs up for our first- party products and services. However,** these ~~sources~~ **checks have failed from time to time and may again fail in the future, and fraud, which may be significant, has and may in the future occur. The level of fraud- related charge- offs on the first- party products and services facilitated through our platform could be adversely affected if fraudulent activity were to significantly increase. We may not be able to recoup funds associated with our first- party products and services made in connection with inaccurate statements, omissions of fact or fraud, in which case our revenue, results of operations,**

profitability and cash flows will be harmed. High profile fraudulent activity or significant increases in fraudulent activity could also lead to regulatory intervention, negative publicity and the erosion of trust from our customers, which could negatively impact our results of operations, brand and reputation, and require us to take steps to reduce fraud risk, which could increase our costs. Information security risks in the financial services industry in particular are significant, in part because of new technologies, the use of the internet and telecommunications technologies (including mobile devices) to conduct financial and other business transactions and the increased sophistication and activities of organized criminals, perpetrators of fraud, hackers, terrorists and other malicious third parties. Recently, there have been **a number of well- publicized attacks or breaches affecting companies** in **the financial services industry, such as the large- scale attacks by foreign nation state actors and a significant uptick in ransomware / extortion attacks at** ~~the~~ **other** ~~past~~ **companies, that have caused heightened concern by customers, and which may also intensify regulatory focus, cause customers to lose trust in the security of the industry in general and result in reduced use of our services and increased costs, all of which could also have a material adverse effect on our business. Given the digital nature of our platform, we are** ~~and~~ **an** ~~may~~ **attractive target and expect to** continue to be ~~subject to cybersecurity events that could materially harm our reputation and~~ **an attractive** ~~future sales. We expect to continue to be a~~ target of attacks specifically designed to impede the performance and availability of our offerings and harm our reputation as a leading cyber security company. In addition, we face the risk of cyberattacks by nation- states and state- sponsored actors, which may increase or heighten due to geopolitical tensions. These attacks may target us, our partners, suppliers, vendors or customers. Similarly, experienced computer programmers or other sophisticated individuals or entities, including malicious hackers, state- sponsored organizations, and insider threats including actions by employees and third- party service providers, have attempted to penetrate, and in some cases have penetrated, our network security or the security of our vendors or suppliers. Such attempts are increasing in number and in technical sophistication, including through the use of AI, and have in the past and could in the future expose us and the affected parties, to risk of loss or misuse of proprietary, personal or confidential information or disruptions of our business operations. **ability** to attract and maintain customers as well as strategic partners,cause us to suffer negative publicity or damage to our brand,and subject us to legal claims and liabilities or regulatory penalties.In addition,unauthorized parties might alter information in our databases,which would adversely affect both the reliability of that information and our ability to market and perform our services as well as undermine our ability to remain compliant with relevant laws and regulations.Techniques used to obtain unauthorized access or to sabotage systems change frequently,are constantly evolving and generally are difficult to recognize and react to effectively ~~,and are increasingly becoming more sophisticated and harder to detect due to the use of " deepfakes ",voice imitation technology and other AI tools~~ . **We** ~~Despite our efforts,we~~ are not always able to anticipate these techniques or to implement adequate or timely preventive or reactive measures. **Several recent** ~~Our brands and their third- party service providers from time to time have experienced and may in the future continue to experience such instances~~ , **highly publicized data** ~~and we may experience heightened risks of cyberattacks and other~~ security breaches ~~or disruptions~~ **,such** as **the large- scale attacks by foreign nation state actors,the global incident involving the MOVEit file transfer software,and** a ~~result of~~ **significant uptick in ransomware / extortion attacks at** ~~the~~ **other** ~~ongoing unification efforts to integrate certain legacy IT infrastructure~~ **companies,have heightened consumer awareness of this issue** and **may embolden individuals or groups to target our** systems **or those** of **our strategic partners or enterprise customers** ~~MALKA and Even Financial Inc. (now Engine by MoneyLion)~~ .Threat actors have previously and could in the future exploit a new vulnerability before we complete our remediation work or identify a vulnerability that we did not effectively remediate.If that happens,there could **be unauthorized access to,or acquisition of,data we maintain,and damage to our systems.We could also face legal action from individuals,** In addition, our internal IT environment continues to evolve. We embrace new ways of sharing data and communicating internally and with partners and customers using methods such as social networking and other consumer-oriented technologies. **The** ~~We also remain vigilant with the~~ increasing use of ~~generative~~ **Gen** AI models in our internal systems which may create new attack methods for adversaries. Our business policies and internal security controls may not keep pace with these changes as new threats emerge, or ~~emerging~~ **new** cybersecurity regulations **emerge** in jurisdictions worldwide. ~~When~~ **Finally, the software upon which we rely may from time to time contain undetected technical errors or bugs, which may only be discovered after the code has been released for external or internal use. Technical errors or other design defects within the software upon which we rely may result in** a **negative experience** ~~data breach occurs, our information technology systems and infrastructure can be subject to damage, compromise, disruption, and shutdown due to attacks or~~ **for customers** ~~breaches by hackers or other circumstances~~ , **clients** ~~such as error or malfeasance by employees~~ or third- party **partners and issues in our provision of our products and** ~~service~~ **services** ~~providers~~ **or their functionality** , **failure to accurately predict or evaluate the suitability of new and existing customers** ~~phishing, social engineering, account takeovers, vulnerability exploitation, misconfigurations, ransomware, or~~ **for** ~~technology malfunction. A~~ **our products and services, failure to comply with applicable laws and regulations, failure to detect fraudulent activity on our platform, delayed introductions of new features or enhancements or failure to protect consumer** data ~~breach may~~ **, our intellectual property or other sensitive data or proprietary information. Any technical errors, bugs or defects discovered in the software upon which we rely could** result in ~~significant legal, financial, and reputational~~ harm ~~, including government inquiries, enforcement actions, litigation, and negative publicity. A series of breaches may be determined~~ to **our reputation** ~~be material at a later date in the aggregate~~ , **loss** ~~even if they may not be material individually at the time~~ of **customers, clients or** ~~their~~ - **third** ~~occurrence. The occurrence~~ **- party partners, increased regulatory scrutiny, fines or penalties, loss** of **revenue or liability for damages,** any of **which** ~~these events, as well as a failure to promptly remedy them when they occur, could compromise our systems and the information stored in our systems. Any such circumstance~~ could adversely affect our ability to attract and maintain customers as..... also face legal action from individuals, business ~~partners~~ , **financial condition** ~~and regulators in connection with data breaches~~ , ~~which would result~~ **results** ~~in increased costs and fees incurred in our defense against those proceedings, and / or~~

~~payment~~ of ~~any regulatory penalties~~ **operations and cash flows** . We collect, use, disclose, store or otherwise process personal information **and other sensitive data** , which **is** ~~subjects~~ **subject** ~~us~~ to ~~privacy~~ **stringent** and ~~data security~~ **changing state and federal** laws **,** and **regulations** ~~contractual commitments~~ . ~~We~~ **In connection with the operation of our business, particularly in relation to our identity and information protection service and financial technology offerings, we** collect, use, process, store, transmit or disclose (collectively, process) an increasingly large amount of confidential information, including personal information (which includes credit card information and other critical data **)** from employees and customers ~~),~~ in **multiple jurisdictions** ~~connection with the operation of our business, particularly in relation to our identity and information protection service offerings~~ . The confidential and personal information we process is subject to an increasing number of federal, state, local and foreign laws regarding privacy ~~and~~ **,** data security **and the collection, and handling of PII and sensitive data** , as well as contractual commitments **, and this regulatory framework is rapidly evolving and likely to remain uncertain for the foreseeable future** . **For example, at the federal level, the GLBA (along with its implementing regulations) requires disclosures to consumers about our handling of their nonpublic personal information and empowers consumers to place restrictions on, or opt out of, our sharing nonpublic personal information with affiliated and nonaffiliated their parties for various purposes. Additionally, our investment adviser, ML Wealth, and broker- dealer, MoneyLion Securities LLC, are subject to SEC Regulation S- P, which requires that covered institutions maintain certain policies and procedures addressing the protection of consumer information and records. At the state level, the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (CCPA) requires certain companies that collect, use, retain, share or sell personal information relating to California consumers to make disclosures to such consumers about their data collection, use, sharing and selling practices, provide such consumers with rights to know, correct and delete personal information relating to them, allow such consumers to opt out of the sale of their personal information or the use of their personal data for cross- context behavioral advertising or automated decision making, and provide such consumers with the right to limit the use and disclosure of certain of their sensitive personal information, all of which could impact our business. The CCPA provides for civil penalties for violations, as well as provides a private right of action for certain data breaches that result in the loss of personal information of California consumers. It remains unclear how various provisions of the CCPA and its regulations will be interpreted and enforced. In addition, other U. S. states have enacted comprehensive privacy laws and regulations providing data privacy rights to their respective residents that could impact our business, which laws may lead other U. S. states or even the U. S. Congress to pass comparable legislation. These new laws may result in additional uncertainty and require us to incur additional costs and expenses in our effort to comply. Additionally, the Federal Trade Commission (the FTC) and many state attorneys general are interpreting federal and state consumer protection laws to impose standards for the online collection, use, dissemination, and security of data. The burdens imposed by the new state privacy laws and other similar laws that may be enacted at the federal and state level may require us to modify our data processing practices and policies, adapt our goods and services and incur substantial expenditures in order to comply** Any failure or perceived failure by us to comply with such obligations has previously and may in the future result in governmental enforcement actions, fines, litigation **(including class actions)** or public statements against us by consumer advocacy groups or others and could cause our customers to lose trust in us, which could have an adverse effect on our reputation and business **. Global privacy and data protection legislation and enforcement are rapidly expanding and evolving, and may be inconsistent from jurisdiction to jurisdiction. We may be or become subject to data localization laws mandating that data collected in a foreign country be processed and stored only or primarily within that country, which may require us to expand our data storage facilities there or build new ones in order to comply. The expenditure this would require, as well as costs of compliance generally, could harm our financial condition** . Additionally, changes to applicable privacy or data security laws could impact how we process personal information and therefore limit the effectiveness of our solutions or our ability to develop new solutions. **Because** ~~For example,~~ the **interpretation and application of many privacy and** ~~European Union General Data Protection Regulation imposes more stringent~~ data protection **laws** ~~requirements and provides for greater penalties for noncompliance of up to the greater of € 20 million or four percent of our worldwide annual revenues. Data protection legislation~~ is ~~also increasing in~~ **uncertain, it is possible that** ~~the~~ **these laws may be interpreted** ~~U. S. at both the federal~~ and ~~state level.~~ **applied in a manner that is inconsistent with our existing data management practices** ~~For~~ **or** ~~example,~~ the ~~California~~ **features of our products and services and platform capabilities. If so, in addition to the possibility of fines, lawsuits, regulatory investigations, government actions,** ~~Consumer~~ **consumer and merchant actions** ~~Privacy Act of 2018 (the CCPA) requires~~ , ~~among~~ **and** other **claims** ~~things, covered companies to provide disclosures to California consumers regarding the use of personal information, gives California residents expanded rights to access their personal information that has been collected and allows such consumers new abilities to opt- out of certain sales of personal information. Further, the California Privacy Rights Act (the CPRA) significantly modifies the CCPA and there are new similar and overlapping state privacy laws in at least 10 other U. S. states, which all go into effect by January 1, 2026. These new laws may result in additional uncertainty and require us to incur additional costs and expenses in our effort to comply. Additionally, the Federal Trade Commission (the FTC) and many state attorneys general are interpreting federal and state consumer protection laws to impose standards for the online collection, use, dissemination, and security of data. The burdens imposed by the new state privacy laws and other similar laws that may be enacted at the federal and state level may require us to modify our data processing practices and policies, adapt our goods and services and incur substantial expenditures in order to comply. Global privacy and data protection legislation and enforcement are rapidly expanding and evolving, and may be inconsistent from jurisdiction to jurisdiction. We may be or become subject to data localization laws mandating that data collected in a foreign country be processed and stored only or primarily within that country. If any country in which we have customers were to adopt a data localization law~~ , we could be required to **fundamentally change** ~~expand our data storage facilities there or~~ **our business activities and practices** ~~build new ones in order~~

~~to comply. The expenditure this would require, as well as costs of compliance generally, could harm our~~ **or modify** ~~financial condition. Additionally, third parties with whom we work, such as vendors or~~ **our** ~~developers~~ **platform** , **which** ~~may violate applicable laws or our policies and such violations can place the personal information of our customers at risk. In addition, our customers may also accidentally disclose their passwords or store them on a device that is lost or stolen, creating the perception that our systems are not secure against third- party access. This~~ could have an adverse effect on our ~~reputation and~~ business. ~~In addition~~ **Any violations or perceived violations of these laws** , ~~such~~ **rules and regulations by us, or any** third parties **with which we do business, may require us to change our business practices or operational structure, including limiting our activities in certain states and / or jurisdictions, addressing legal claims by governmental entities or private actors, sustaining monetary penalties, sustaining reputational damage, expending substantial costs, time and other resources and / or sustaining other harms to our business. Furthermore, our online, external- facing privacy policy and website make certain statements regarding our privacy, information security and data security practices with regard to information collected from our consumers or visitors to our website. Failure or perceived failure to adhere to such practices may result in regulatory scrutiny and investigation, complaints by affected consumers or visitors to our website, reputational damage and / or other harm to our business. If either we, or the third- party partners, service providers or vendors with which we share consumer data, are unable to address privacy concerns, even if unfounded, or to comply with applicable privacy or data protection laws, regulations and policies, it** could ~~expose~~ **result in additional costs and liability to** us **, damage** ~~to compromised data or~~ **our** ~~technology~~ **reputation** , **inhibit sales and harm** ~~or~~ **our business** ~~be the target of cyberattack and other data breaches which could impact our systems or our customers' records and personal information. Further~~ , **financial condition,** ~~we could be the target of a cyberattack or other action that impacts our systems and~~ results ~~in a data breach~~ of **operations** ~~our customers' records and personal information. This could have an~~ **and cash flows** ~~adverse effect on our reputation and business and potentially result in litigation and / or regulatory penalties~~ . Our inability to successfully recover from a disaster or other business continuity event could impair our ability to deliver our products and services and harm our business. We are heavily reliant on our technology and infrastructure to provide our products and services to our customers **. We use third- party service providers and vendors, such as our cloud computing web services provider, account transaction and card processing companies, in the operation of certain of our platforms and we source certain information from third- parties** . For example, we host many of our products using third- party data center facilities and we do not control the operation of these facilities. These facilities are vulnerable to damage, interference, interruption or performance problems from earthquakes, hurricanes, floods, fires, power loss, telecommunications failures, pandemics and similar events. They are also subject to break- ins, computer viruses, sabotage, intentional acts of vandalism and other misconduct. The occurrence of a natural disaster, an act of terrorism state- sponsored attacks, a pandemic, geopolitical tensions or armed conflicts, and similar events could result in a decision to close the facilities without adequate notice or other unanticipated problems, which in turn, could result in lengthy interruptions in the delivery of our products and services, which could negatively impact our sales and operating results. **If an arrangement with a third- party service provider or vendor is terminated or if there is a lapse of service or damage to its systems or facilities, we could experience interruptions in our ability to operate our platform. We also may experience increased costs and difficulties in replacing that third- party service provider or vendor, and replacement services may not be available on commercially reasonable terms, on a timely basis, or at all. In the event of damage or interruption, our insurance policies may not adequately compensate us for any losses that we may incur.** Furthermore, our business administration, human resources, compliance efforts and finance services depend on the proper functioning of our computer, telecommunication and other related systems and operations **, which are highly technical and complex** . A disruption or failure of these systems or operations because of a disaster, cyberattack or other business continuity event, such as a pandemic, could cause data to be lost or otherwise delay our ability to complete sales and provide the highest level of service to our customers. In addition, we could have difficulty producing accurate financial statements on a timely basis, and deficiencies may arise in our internal control over financial reporting, which may impact our ability to certify our financial results, all of which could adversely affect the trading value of our stock. There are no assurances that data recovery in the event of a disaster would be effective or occur in an efficient manner. If these systems or their functionality do not operate as we expect them to, we may be required to expend significant resources to make corrections or find alternative sources for performing these functions ~~. We are dependent upon Broadcom for certain engineering and threat response services, which are critical to many of our products and business~~ . Our Norton branded endpoint security solution has historically relied upon certain threat analytics software engines and other software (the Engine- Related Services) that have been developed and provided by engineering teams that have transferred to Broadcom as part of the Broadcom sale. The technology, including source code, at issue is shared, and pursuant to the terms of the Broadcom sale, we retain rights to use, modify, enhance and create derivative works from such technology. Broadcom has committed to provide these Engine- Related Services substantially to the same extent and in substantially the same manner, as has been historically provided under a license agreement with a limited term. As a result, we are dependent on Broadcom for services and technology that are critical to our business, and if Broadcom fails to deliver these Engine- Related Services it would result in significant business disruption, and our business and operating results and financial condition could be materially and adversely affected. Furthermore, if our current sources become unavailable, and if we are unable to develop or obtain alternatives to integrate or deploy them in time, our ability to compete effectively could be impacted and have a material adverse effect on our business. Additionally, in connection with the Broadcom sale, we lost other capabilities, including certain threat intelligence data which were historically provided by our former Enterprise Security business, the lack of which could have a negative impact on our business and products. ~~If we fail to offer high- quality customer support, our customer satisfaction may suffer and have a negative impact on our business and reputation.~~ Many of our customers rely on our customer support services to resolve issues, including technical support, billing and subscription issues, that may arise. If demand increases, or our resources decrease, we may be unable to offer the level of

support our customers expect. Any failure by us to maintain the expected level of support could reduce customer satisfaction and negatively impact our customer retention and our business ~~. Our solutions are complex and operate in a wide variety of environments, systems and configurations, which could result in failures of our solutions to function as designed~~ . Because we offer very complex solutions, errors, defects, disruptions, or other performance problems with our solutions may occur and have occurred. For example, we may experience disruptions, outages and other performance problems due to a variety of factors, including infrastructure changes, human or software errors, fraud, security attacks or capacity constraints due to an overwhelming number of users accessing our websites simultaneously **. As we continue to expand the number of our customers and the products and services available through our platform, we may not be able to scale our technology to accommodate the increased capacity requirements. The failure of data centers, internet service providers or other third-party service providers or vendors to meet our capacity requirements could result in interruptions or delays in access to our platform or impede our ability to grow our business and scale our operations** . In some instances, we may not be able to identify the cause or causes of these performance problems within an acceptable period of time. Interruptions in our solutions could impact our revenues **, prevent** ~~or~~ **our customers from accessing their accounts, damage our reputation with current and potential customers, expose us to liability,** cause **us to lose** customers ~~to~~ **,** ~~cease~~ **cause** ~~doing~~ **the loss of critical data or personal information, prevent us from supporting our platform, products or services or processing transactions with our customers or cause us to incur additional expense in arranging for new facilities and support or otherwise harm our** business **, any of which** ~~with us. Our operations are dependent upon our ability to protect our technology infrastructure against damage from business continuity events that~~ could have a ~~significant disruptive~~ **material and adverse** effect on our **business, financial condition, results of** operations **and cash flows** ~~. We could potentially lose customer data or personal information, or experience material adverse interruptions to our operations or delivery of solutions to our clients~~ in a disaster recovery scenario. ~~Negative publicity regarding~~ **To the extent we use** ~~our~~ **or** ~~brand~~ **are dependent on any particular third- party data** , ~~solutions and business~~ **technology or software, we may also be harmed if such data, technology, or software becomes non-compliant with existing regulations or industry standards, becomes subject to third- party claims of intellectual property infringement, misappropriation or other violation, or malfunctions or functions in a way we did not anticipate. Any loss of the right to use any of this data, technology or software** could ~~harm~~ **result in delays in the provisioning of our products and services until equivalent** ~~our~~ **or** ~~competitive position~~ **replacement data, technology or software is either developed by us, or, if available, is identified, obtained and integrated, and there is no guarantee that we would be successful in developing, identifying, obtaining or integrating equivalent or similar data, technology or software, which could result in the loss or limiting of our products or services or features available in our products or services** . Our brand recognition and reputation as a trusted service provider are critical aspects of our business and key to retaining existing customers and attracting new customers. Our business could be harmed due to errors, defects, disruptions or other performance problems with our solutions causing our customers and potential customers to believe our solutions are unreliable. **We may introduce, or make changes to, features, products, services, privacy practices or terms of service that customers and clients do not like, which may materially and adversely affect our brand. Our efforts to build our brand have involved significant expense, and our marketing spend may increase in the near term or in the future and may not generate or maintain brand awareness or increase revenue. Due to unfamiliarity and negative publicity associated with digital asset- related businesses, existing and potential customers may lose confidence in our digital asset- related products and services, which could negatively affect our reputation and business.** Furthermore, negative publicity, whether or not justified, including intentional brand misappropriation, relating to events or activities attributed to us, our employees, our strategic partners, our affiliates, or others associated with any of these parties, may tarnish our reputation and reduce the value of our brands ~~. In addition, the rapid rise and use of social media has the potential to harm our brand and reputation. We may be unable to timely respond to and resolve negative and inaccurate social media posts regarding our company, solutions and business in an appropriate manner~~ . Damage to our reputation and loss of brand equity may reduce demand for our solutions and have an adverse effect on our business, operating results and financial condition. Moreover, any attempts to rebuild our reputation and restore the value of our brands may be costly and time consuming, and such efforts may not ultimately be successful. ~~Our reputation and / or business could be negatively impacted by ESG matters and / or our reporting of such matters.~~ The **evolving** focus from regulators, customers, certain investors, employees, and other stakeholders concerning **sustainability** ~~environmental, social~~ and governance ~~(ESG)~~ matters and related disclosures, both in the United States and internationally, has resulted in, and is likely to continue to result in, increased general and administrative expenses and increased management time and attention spent complying with or meeting ~~ESG~~ **sustainability** - related requirements and expectations. For example, developing and acting on ~~ESG~~ **sustainability** - related initiatives and collecting, measuring and reporting ~~ESG~~ **sustainability** - related information and metrics can be costly, difficult and time consuming and is subject to evolving reporting standards, including ~~the SEC' s climate-related reporting requirements and~~ the recent California legislation, which includes disclosure requirements relating to voluntary carbon offsets and a wide range of environmental marketing claims. Similarly, the Corporate Sustainability Reporting Directive will require large EU companies to make detailed disclosures in relation to certain sustainability- related issues. We ~~communicate~~ **maintain** certain ~~ESG~~ **sustainability** - related initiatives, goals, and / or commitments ~~regarding environmental matters, diversity, responsible sourcing and social investments and other matters on our website, in our filings with the SEC and elsewhere~~ . These initiatives, goals or commitments could be difficult to achieve and costly to implement, the technologies needed to implement them may not be cost effective and may not advance at a sufficient pace, and we could be criticized for the accuracy, adequacy or completeness of the disclosure. Further, statements about our ~~ESG~~ **sustainability** - related initiatives, goals or commitments and progress with respect to such initiatives, goals or commitments may be based on standards for measuring progress that are still developing, internal controls and processes that continue to evolve, and assumptions that are subject to change in the future. In addition, we could be criticized for the timing, scope or nature of these initiatives, goals or

commitments, or for any revisions to them. If we fail to achieve progress with respect to our ~~ESG~~ **sustainability** - related initiatives, goals or commitments on a timely basis, or at all, or if our ~~ESG~~ **sustainability** - related data, processes and reporting are incomplete or inaccurate, our reputation, business, financial performance and growth could be adversely affected. **Additionally changing federal enforcement priorities** ~~We are affected by seasonality, which may impact our revenue~~ and ~~results of operations~~ **legal interpretations regarding diversity, equity, and inclusion programs present unknown and evolving risks** . Portions of our business are impacted by seasonality. Seasonal behavior in orders has historically occurred in the third and fourth quarters of our fiscal year, which include the important selling periods during the holidays in our third quarter, as well as follow- on holiday purchases and the U. S. tax filing season, which is typically in our fourth quarter. Revenue generally reflects similar seasonal patterns, but to a lesser extent than orders. This is due to our subscription business model, as a large portion of our in- period revenue is recognized ratably from our deferred revenue balance. An unexpected decrease in sales over those traditionally high- volume selling periods may impact our revenue and could have a disproportionate effect on our results of operations for the entire fiscal year. **RISKS RELATED TO** LEGAL AND COMPLIANCE ~~RISKS~~ Our solutions are highly regulated, which could impede our ability to market and provide our solutions or adversely affect our business, financial position ~~and~~ **,** results of operations **and cash flows** . Our solutions are subject to a high degree of regulation, including a wide variety of international and U. S. federal, state, and local laws and regulations, such as the Fair Credit Reporting Act, the Gramm- Leach- Bliley Act, the Federal Trade Commission Act (the FTC Act), and comparable state laws that are patterned after the FTC Act **, the U. S. Foreign Corrupt Practices Act of 1977, U. S. domestic bribery laws and other U. S. and foreign anti- corruption laws. We maintain an enterprise- wide compliance program designed to enable us to comply with all applicable anti- money laundering, anti- terrorism financing and economic sanctions laws and regulations, including the BSA, as amended by the USA PATRIOT Act of 2001, and its implementing regulations. This compliance program includes policies, procedures, processes and other internal controls designed to identify, monitor, manage and mitigate the risk of money laundering and terrorist financing and prevent our platform from being used to facilitate business in countries or with persons or entities that are the subject of sanctions administered by OFAC and equivalent international authorities or that are otherwise the target of sanctions. These controls include procedures and processes to detect and report potentially suspicious transactions, perform customer due diligence, respond to requests from law enforcement and meet all recordkeeping and reporting requirements related to particular transactions involving currency or monetary instruments. Certain of our subsidiaries may be " financial institutions " under the BSA that are required to establish and maintain a BSA / AML compliance program. Additionally, we are required to maintain a BSA / AML compliance program under our agreements with our third- party partners, and certain state regulatory agencies have intimated they expect such program to be in place and followed** . We have ~~previously~~ **in the past, and may again in the future,** ~~entered~~ -- **enter** into **settlements,** consent decrees and similar arrangements with the FTC ~~and the~~ **, state** attorney generals ~~of 35 states as well as a settlement with the FTC relating to allegations that certain of LifeLock' s advertising~~ , ~~marketing and security practices constituted deceptive acts or practices in violation of the FTC Act, which impose additional restrictions on our business, including prohibitions against making any misrepresentation of " the means, methods, procedures, effects, effectiveness, coverage, or scope of " our solutions. We signed an~~ **and** ~~Undertaking, effective June 14, 2021, with~~ the United Kingdom' s Competition and Markets Authority (CMA) ~~requiring our NortonLifeLock Ireland Limited~~ **. We must comply with various federal** and **state consumer protection regimes, both** ~~NortonLifeLock UK entities to make certain changes to their policies and practices related to automatically renewing subscriptions in the United Kingdom~~ as ~~part~~ **a result** of the **financial products** ~~CMA' s investigation into auto- renewal practices in the antivirus sector launched in December 2018. Any of the laws~~ and **services** ~~regulations that apply to our business are subject to revision or new or changed interpretations, and~~ we **provide directly** ~~cannot predict the impact of such changes on our~~ - **or** ~~business~~ **facilitate and as a service provider to our bank partner, Pathward** . Additionally, the nature of our **MoneyLion,** identity **,** and information protection products subjects us to the broad regulatory, supervisory and enforcement powers of the Consumer Financial Protection Bureau which may exercise authority with respect to our services, or the marketing and servicing of those services, through the oversight of our financial institution or credit reporting agency customers and suppliers, or by otherwise exercising its supervisory, regulatory or enforcement authority over consumer financial products and services. **Additionally, we are regulated by many state regulatory agencies through licensing and other supervisory or enforcement authority, which includes regular examination by state governmental authorities. U. S. federal regulators, state attorneys general or other state enforcement authorities and other governmental agencies may take formal or informal actions again in cease and desist orders, fines, civil penalties, criminal penalties or other disciplinary action or force us to adopt new compliance programs or policies, remove personnel including senior executives, provide remediation or refunds to customers, or undertake other changes to our business operations, such as limits or prohibitions of our ability to offer certain products and services, or suspension or revocation of one or more of our licenses. Any weaknesses in our compliance management system may also subject us to penalties or enforcement action by the CFPB. In addition, certain products and offers we offer, including loans facilitated through our platform, could be rendered void or unenforceable in whole or in part, which could adversely affect our business, financial condition, results of operations and cash flows. Additionally, the highly regulated environment in which our third- party financial institution partners operate may subject us to regulation and could have an adverse effect on our business, financial condition, results of operations and cash flows** If **we fail to manage our legal and regulatory risk in the jurisdictions in which we operate, our business could suffer, our reputation could be harmed and we would be subject to additional legal and regulatory risks. This could, in turn, increase the size and number of claims and damages asserted against us and / or subject us to regulatory investigations, enforcement actions or other proceedings, or lead to increased regulatory concerns. We may also be required to spend additional time and resources on remedial measures and conducting inquiries, beyond those already initiated and**

ongoing, which could have an adverse effect on our business. We have in the past, and continue to be, subject to inquiries, subpoenas, exams, pending investigations, enforcement matters and litigation by state and federal regulators, the outcomes of which are uncertain and could cause reputational and financial harm to our business, financial condition, results of operations and cash flows. For a discussion of specific legal and regulatory proceedings, inquiries and investigations to which we are currently subject, see Note 18 of the Notes to the Consolidated Financial Statements included in this Annual Report on Form 10- K. The legal and regulatory regimes governing certain of our products and services are uncertain and evolving. Changing or new laws, regulations, interpretations or regulatory enforcement priorities may have a material and adverse effect on our business, financial condition, results of operations and cash flows. Changes in the laws, regulations and enforcement priorities applicable to our business, including reexamination of current enforcement practices, could have a material and adverse impact on our business, financial condition, results of operations and cash flows. We and / or our third- party partners may not be able to respond quickly or effectively to regulatory, legislative and other developments. We cannot determine with any degree of certainty whether any legislative or regulatory changes will be enacted and, if enacted, the ultimate impact that any such potential legislation or implemented regulations, or any such potential regulatory actions by federal or state regulators, would have upon our business or our operating environment. These changes and uncertainties make our business planning more difficult and could result in changes to our business model, impair our ability to offer our existing or planned features, products and services or increase our cost of doing business. New laws, regulations, rules, guidance and policies could require us to incur significant expenses to ensure compliance, adversely impact our profitability, limit our ability to continue existing or pursue new business activities, require us to change certain of our business practices or alter our relationships with customers, affect retention of key personnel or expose us to additional costs (including increased compliance costs and / or customer remediation). For example, the regulatory frameworks for an open banking paradigm and AI and machine learning technology are evolving and remain uncertain. It is possible that new laws and regulations will be adopted in the U. S., or existing laws and regulations may be interpreted in new ways, that would affect the operation of our platform and the way in which we use consumer data, AI and machine learning technology, including with respect to fair lending laws. For additional information regarding risks related to the use of AI, see"--- Issues in the development and deployment of artificial intelligence (“ AI ”) may result in reputational harm and legal liability and could adversely affect our results of operations. ” If loans made by our lending subsidiaries in our Consumer business are found to violate applicable federal or state interest rate limits or other provisions of applicable consumer lending, consumer protection or other laws, it could adversely affect our business, financial condition, results of operations and cash flows. In our Consumer business, we have 37 subsidiaries through which we conduct our consumer lending business. These entities originate loans pursuant to state licenses or applicable exemptions under state law. The loans we originate are subject to state licensing or exemption requirements and federal and state interest rate restrictions, as well as numerous federal and state requirements regarding consumer protection, interest rate, disclosure, prohibitions on certain activities and loan term lengths. If the loans we originate were deemed subject to and in violation of certain federal or state consumer finance or other laws, including the Military Lending Act, we could be subject to fines, damages, injunctive relief (including required modification or discontinuation of our business in certain areas) and other penalties or consequences, and the loans could be rendered void or unenforceable in whole or in part, any of which could have an adverse effect on our business, financial condition, results of operations and cash flows. For a discussion of the ongoing civil action initiated by the CFPB alleging certain violations of the Military Lending Act and the Consumer Financial Protection Act, see Note 18 of the Notes to the Consolidated Financial Statements included in this Annual Report on Form 10- K. The regulatory regime governing blockchain technologies and digital assets is uncertain, and new laws, regulations or policies may alter our business practices with respect to digital assets. We currently offer certain digital assets- related products and services available to our customers through Zero Hash. The Zero Hash entities are registered as money services businesses. Although many regulators have provided some guidance, regulation of digital assets based on or incorporating blockchain technologies, such as digital assets and digital asset exchanges, remains uncertain and will continue to evolve. Further, regulation varies significantly among international, federal, state and local jurisdictions. As blockchain networks and blockchain assets have grown in popularity and in market size, federal and state agencies are increasingly taking interest in, and in certain cases regulating, their use and operation. Treatment of virtual currencies, including digital assets, continues to evolve under federal and state law. Many U. S. regulators, including the SEC, the FinCEN, the Commodity Futures Trading Commission (the “ CFTC ”), the Internal Revenue Service (the “ IRS ”) and state regulators including the New York State Department of Financial Services (the “ NYSDFS ”), have made official pronouncements, pursued cases against businesses in the digital assets space or issued guidance or rules regarding the treatment of Bitcoin and other digital currencies. The IRS released guidance treating digital assets as property that is not currency for U. S. federal income tax purposes. Additionally, many other aspects of the U. S. and foreign tax treatment of transactions involving digital assets are uncertain, and it is unclear whether, when and what guidance may be issued in the future on the treatment of digital asset transactions for U. S. and foreign tax purposes. Both federal and state agencies have instituted enforcement actions against those violating their interpretation of existing laws. Other U. S. and many state agencies have offered little official guidance and issued no definitive rules regarding the treatment of digital assets. The CFTC has publicly taken the position that certain virtual currencies, including digital assets, are commodities. To the extent that certain virtual currencies, including digital assets, are deemed to fall within the definition of a “ commodity interest ” under the Commodity Exchange Act (the “ CEA ”), or if proposed legislation passes which grants the CFTC jurisdiction over spot digital asset trading beyond its current limited power to bring actions for fraud and manipulation, we may be subject to additional regulation under the CEA and

CFTC regulations. Foreign, federal, state and local regulators revisit and update their laws and policies on blockchain technologies and digital assets and can be expected to continue to do so in the future. Regulatory or enforcement action in this area have been common. As we facilitate our customers' purchase and sale of digital assets, if the SEC alleges that any digital assets we offer are securities, we could be viewed as operating as an unregistered broker- dealer and could face potential liability, including an enforcement action or private class action lawsuits, and face the costs of defending ourselves in the action, including potential fines, penalties, reputation harm and potential loss of revenue. Our personnel could also become disqualified from associating with a broker- dealer, which could adversely affect our business. States may require that we obtain licenses that apply to blockchain technologies and digital assets. Under the terms of our agreement with Zero Hash, we are not directly involved in any digital asset transactions or the exchange of fiat funds for digital asset at or through Zero Hash, and therefore, we do not ~~protect~~ **currently expect to be subject to money services business, money transmitter licensing** ~~our~~ **or** ~~proprietary information~~ **other licensing or regulatory requirements specific to transactions relating to virtual currencies. However, state and federal regulatory frameworks around virtual currencies, including digital assets, continue to evolve and are subject to interpretation and change, which may subject us to additional licensing and other requirements. The Zero Hash entities are registered as money services businesses with FinCEN and hold active money transmitter licenses (or the state equivalent of such licenses) in all U. S. states and the District of Columbia except for (i) California and Hawaii, where Zero Hash relies upon licensing exemptions; and (ii) Montana, which does not currently have a money transmitter licensing requirement. The Zero Hash entities currently engage in digital asset activities in all U. S. states and the District of Columbia. Zero Hash is the custodian of all customer digital assets. It uses both multi- party computation (i. e., " warm ") and cold omnibus wallets, generally on a per asset basis, and Zero Hash holds** ~~and~~ **an inventory of digital assets in omnibus wallets for the purpose of providing customers instant access to purchased digital assets. Zero Hash has a custodial agreement with Coinbase Trust Company, LLC, which is based in the State of New York, for the provision of cold wallet storage and related services. As we are not directly involved in the custody, trading or pricing of any digital assets and, instead, enable Zero Hash to offer its digital asset services to MoneyLion Crypto customers, we do not maintain insurance policies covering the digital assets in which MoneyLion Crypto customers transact. In addition, our agreement with Zero Hash does not require Zero Hash to indemnify us or MoneyLion Crypto customers for any risk of loss related to customers' underlying digital assets, nor does it require Zero Hash to maintain an insurance policy with respect to the digital assets of MoneyLion Crypto customers custodied with Zero Hash. Zero Hash does not maintain separate insurance coverage for any risk of loss with respect to the digital assets that they custody on behalf of customers. As a result, customers who purchase digital assets through MoneyLion Crypto may suffer losses with respect to their digital assets that are not covered by insurance and for which no person is liable for damages and may have limited rights of legal recourse in the** ~~prevent~~ **event** ~~third parties~~ **of such loss. In the case of virtual currencies, state regulators such as the NYSDFS have created regulatory frameworks. For example, in July 2014, the NYSDFS proposed the first U. S. regulatory framework for licensing participants in digital asset business activity. The regulations, known as the " BitLicense " (23 NYCRR Part 200), are intended to focus on consumer protection. The NYSDFS issued its final BitLicense regulatory framework in June 2015. The BitLicense regulates the conduct of businesses that are involved in virtual currencies in New York or with New York consumers and prohibits any person or entity involved in such activity** from ~~making unauthorized~~ **conducting such activities without a license. Zero Hash LLC has received a BitLicense and is approved to conduct digital asset business activity in New York by the NYSDFS. Other states, such as Louisiana and California, have and may in future adopt similar statutes and regulations which will require us or our partners to obtain a license to conduct digital asset activities. Other states, such as Texas, have published guidance on how their existing regulatory regimes governing money transmitters apply to virtual currencies. Some states, such as Alabama, North Carolina and Washington, have amended their state' s statutes to include virtual currencies in existing licensing regimes, while others have interpreted their existing statutes as requiring a money transmitter license to conduct certain digital asset business activities. It is likely that, as blockchain technologies and the** use of **virtual currencies continues to grow, additional states will take steps to monitor the developing industry and may require us** ~~our~~ **or** ~~products and technology,~~ our ~~financial results could be harmed~~ **regulated partners to obtain additional licenses in connection with our digital asset activity** . Much of our software and underlying technology is proprietary ~~. We seek~~ **, and thus we are highly dependent on our ability** to protect ~~our proprietary rights through a combination of~~ **such technology. There is no guarantee that** confidentiality agreements ~~and~~ **, our** procedures and ~~through~~ copyright, patent, trademark and trade secret laws **will** ~~. However, these measures afford only limited protection and may~~ be ~~challenged, invalidated~~ **sufficient to protect** ~~or~~ **our technology** ~~circumvented by third parties~~ . ~~Third parties may copy all or~~ **For example** ~~portions of our products or otherwise obtain~~ , ~~use, distribute and sell our proprietary information without authorization. Patents~~ **patents** may ~~also~~ not be issued from our pending patent applications and claims allowed on any future issued patents may not be sufficiently broad to protect our technology. Also, these protections may not preclude competitors from independently developing products with functionality or features similar to our products. **These measures afford only limited protection, are costly to maintain and may be challenged, invalidated or circumvented by third parties. Accordingly, enforcement of our intellectual property rights may be difficult, particularly in some countries outside of North America in which we seek to market our software products and services, and the absence of internationally harmonized intellectual property laws or the lack of some laws in certain jurisdictions makes it more difficult to ensure consistent protection of our proprietary rights. For example, software piracy has been, and is expected to be, a persistent problem for the software industry, and a loss of revenue to us. Unauthorized third parties, including our competitors, may reverse engineer, access, obtain, distribute, sell or use the proprietary aspects of our technology, processes, products, information or services without our permission, thereby impeding our ability to promote our**

platform and possibly leading to customer confusion. Third parties have previously and may in the future also develop similar or superior technology independently by designing around our patents. Our consumer agreements do not require a signature and therefore may be unenforceable under the laws of some jurisdictions. ~~Furthermore, the laws of some foreign countries do not offer the same level of protection of our proprietary rights as the laws of the United States, and we may be subject to the unauthorized use of our products in those countries. The unauthorized copying or use of our products or proprietary information could result in reduced sales of our products.~~ Any legal action to protect proprietary information that we may bring or be engaged in with a strategic partner or vendor could adversely affect our ability to access software, operating system and hardware platforms of such partner or vendor, or cause such partner or vendor to choose not to offer our products to their customers. In addition, any legal action to protect proprietary information that we may bring or be engaged in, could be costly, may distract management from day- to- day operations and may lead to additional claims against us, which could adversely affect our operating results. **In addition to registered intellectual property rights such as trademark registrations, we rely on non- registered proprietary information and technology, such as trade secrets, confidential information, know- how and technical information. The secrecy of such trade secrets and other sensitive information could be compromised, which could cause us to lose the competitive advantage resulting from these trade secrets. For example, there is a risk of employees inadvertently inputting trade secret information into Gen AI technologies, thereby enabling third parties, including our competitors, to access such information. We utilize confidentiality and intellectual property assignment agreements with our employees and contractors involved in the development of material intellectual property for us, which require such individuals to assign such intellectual property to us and place restrictions on the employees' and contractors' use and disclosure of our confidential information. However, these agreements may not be self- executing, and we cannot guarantee that we have entered into such agreements containing obligations of confidentiality with each party that has or may have had access to proprietary information, know- how or trade secrets owned or held by us. Additionally, our contractual arrangements may be insufficient, breached or may otherwise not effectively prevent disclosure of, or control access to, our confidential or otherwise proprietary information or provide an adequate remedy in the event of an unauthorized disclosure, which could cause us to lose any competitive advantage resulting from this intellectual property. Individuals that were involved in the development of intellectual property for us or who had access to our intellectual property may make adverse ownership claims to our current and future intellectual property. Likewise, to the extent that our employees, independent contractors or other third parties with whom we do business use intellectual property owned by others in their work for us, disputes may arise as to the rights in related or resulting works of authorship, know- how and inventions. The measures we have put in place may not prevent misappropriation, infringement or other violation of our intellectual property, proprietary rights or information, and any resulting loss of competitive advantage, and we may be required to litigate to protect our intellectual property or other proprietary rights or information from misappropriation, infringement or other violation by others, which is time- consuming and expensive, could cause a diversion of resources and may not be successful. Additionally, our efforts to enforce our intellectual property and other proprietary rights may be met with defenses, counterclaims and countersuits attacking the validity and enforceability of our intellectual property and other proprietary rights, and if such defenses, counterclaims or countersuits are successful, it could diminish, or we could otherwise lose, valuable intellectual property and other proprietary rights. Any of the foregoing could adversely impact our business, financial condition, results of operations and cash flows. In addition, the integration of Gen AI may also expose us to risks regarding intellectual property ownership and license rights, particularly if any copyrighted material is embedded in training models or if the output we produce is infringing intellectual property rights. In addition, the use of Gen AI in connection with the creation or development of intellectual property may present challenges in asserting ownership over the resulting output given the position of some courts and intellectual property offices in various jurisdictions that some human contribution is required for intellectual property protection of an AI- generated work.** From time to time we are party to lawsuits and investigations ~~, and third parties have claimed and additional third parties in the future may claim that we infringe their proprietary rights~~ , which has previously and could in the future require significant management time and attention, cause us to incur significant legal expenses and prevent us from selling our products. We are **, and may in the future become, subject to litigation, claims, examinations, investigations, legal and administrative cases and proceedings, whether civil or criminal, or lawsuits by governmental agencies or private parties, which may affect our business, financial condition, results of operations and cash flows. These claims, lawsuits and proceedings could involve labor and employment, discrimination and harassment, commercial disputes, class actions, general contract, tort, defamation, data privacy rights, antitrust, common law fraud, government regulation, compliance, alleged federal and state securities and " blue sky " law violations or other investor claims and other matters. For a discussion of specific legal proceedings to which we are currently subject. Refer to Note 18 of the Notes to the Consolidated Financial Statements included in this Annual Report on Form 10- K. Due to the consumer- oriented nature of a significant portion of our MoneyLion business and the application of certain laws and regulations, participants in our industry are regularly named as defendants in litigation alleging violations of federal and state laws and regulations and consumer law torts, including fraud. Many of these legal proceedings involve alleged violations of consumer protection laws. In addition, we have in the past and may in the future be subject to litigation, claims, examinations, investigations, legal and administrative cases and proceedings related to our loan products and other financial services we provide. For instance, our membership model and some of the products and services we offer, including our earned wage access product, Instacash, are relatively novel and have been and may in the future continue to be subject to regulatory scrutiny or interest and / or litigation. Any regulatory action in the future could have a material adverse effect on our business, financial condition, results of operations and cash flows. We are also** frequently involved in litigation and other proceedings, including, but not limited to, class actions and

governmental claims or investigations, some of which may be material initially or become material over time. The expense of initiating and defending, and in some cases settling, such matters may be costly and divert management' s attention from the day- to- day operations of our business, which could have a materially adverse effect on our business, results of operations and cash flows. In addition, such matters may through the course of litigation or other proceedings change unfavorably which could alter the profile of the matter and create potential material risk to the company. Any unfavorable outcome in a matter could result in significant fines, settlements, monetary damages, or injunctive relief that could negatively and materially impact our ability to conduct our business, results of operations and cash flows. Additionally, in the event we did not previously accrue for such litigation or proceeding in our financial statements, we may be required to record retrospective accruals that adversely affect our results of operations and financial condition. **Finally, there can be no assurance that we will be able to maintain insurance on acceptable terms in the future, if at all, or that any such insurance will provide adequate protection against potential liabilities.** Additionally, **we do not carry insurance for all categories of risk that our business may encounter. Any significant liability that is uninsured or not fully insured may require us to pay substantial amounts. There can be no assurance that any current or future claims will not materially and adversely affect our business, financial condition, results of operations and cash flows.** ~~third~~ **Third** parties have claimed and, from time to time, additional third parties may claim that we have infringed their intellectual property rights, including claims regarding patents, copyrights and trademarks. For additional information on such claims, please refer to Note 18 of the Notes to the Consolidated Financial Statements included in this Annual Report on Form 10- K. Because of constant technological change in the segments in which we compete, the extensive patent coverage of existing technologies, and the rapid rate of issuance of new patents, it is possible that the number of these claims may grow. In addition, former employers of our former, current or future employees may assert claims that such employees have improperly disclosed to us confidential or proprietary information of these former employers. Any such claim, with or without merit, could result in costly litigation and distract management from day- to- day operations. If we are not successful in defending such claims, we could be required to stop selling, delay shipments of, or redesign our solutions, pay monetary amounts as damages, enter into royalty or licensing arrangements, or satisfy indemnification obligations that we have with some of our partners. We cannot assure you that any royalty or licensing arrangements that we may seek in such circumstances will be available to us on commercially reasonable terms or at all. We ~~have made and expect to continue making significant expenditures to investigate, defend and settle claims related to the use of technology and intellectual property rights as part of our strategy to manage this risk. In addition, we~~ license and use software from third parties in our business and generally must rely on those third parties to protect the licensed rights **and avoid infringement. Third- party software components may become obsolete, defective or incompatible with future versions of our services, or our relationships with the third- party licensors or technology providers may deteriorate, expire or be terminated**. These third- party software licenses may not continue to be available to us on acceptable terms or at all and may expose us to additional liability. **Our inability to obtain licenses or rights on favorable terms could have a material and adverse effect on our business and results of operations. Even if such licenses or other grants of rights are available, we may be required to pay the licensor (or other applicable counterparty) substantial royalties, which may affect the margins on our products and services. Furthermore, incorporating intellectual property or proprietary rights in our products or services licensed from or otherwise made available to us by third parties on a non- exclusive basis could limit our ability to protect the intellectual property and proprietary rights in our products and services and our ability to restrict third parties from developing, selling or otherwise providing similar or competitive technology using the same third- party intellectual property or proprietary rights.** This liability, or our inability to use any of this third- party software, could result in delivery delays or other disruptions in our business that could materially and adversely affect our operating results. **If we fail** ~~Some of our products contain " open source " software, and any failure~~ to comply with **any of the obligations under our license agreements, we may be required to pay damages and the licensor may have the right to terminate the license, which would cause us to lose valuable rights, and could prevent us from selling our products and services, or inhibit our ability to commercialize current or future products and services. Our business may suffer if any current or future licenses or other grants of rights to us terminate, if the licensors (or other applicable counterparties) fail to abide by** the terms of ~~one or more of these -- the open source licenses~~ **license or other applicable agreement, if the licensors fail to enforce the licensed intellectual property rights against infringing third parties, or if the licensed intellectual property rights are found to be invalid or unenforceable. Third parties from whom we currently license intellectual property and technology** could ~~negatively affect~~ **refuse to renew our agreements upon their expiration** ~~our~~ **or** ~~business~~ **could impose additional terms and fees that we otherwise would not deem acceptable, requiring us to obtain the intellectual property or technology from another third party, if any is available, or to pay increased licensing fees or be subject to additional restrictions on our use of such third- party intellectual property or technology**. Certain of our products are distributed with software licensed by its authors or other third parties under so- called " open source " licenses. Some of these licenses contain requirements that we make available source code for modifications or derivative works we create based upon the open source software and that we license such modifications or derivative works under the terms of a particular open source license or other license granting third parties certain rights of further use. By the terms of certain open source licenses, we could be required to release the source code of our proprietary software **(which could include our proprietary source code or AI models)** if we combine our proprietary software with open source software in a certain manner. Some open source software may include **Gen** ~~generative artificial intelligence (~~ AI ~~)~~ software **which** ~~or other software that incorporates or relies on generative AI. The use of such software~~ may expose us to risks as the intellectual property ownership and license rights, including copyright, of ~~generative~~ **Gen** AI software and tools ~~,~~ has not been fully interpreted by U. S. courts or been fully addressed by federal, state, or international regulations. In addition to risks related to license requirements, using open source software, including open source software that incorporates or relies on ~~generative~~ **Gen** AI, can lead to greater risks than use of third- party commercial software, as open source licensors generally do

not provide warranties or controls on origin of the software. We ~~have established processes to help alleviate these risks, including a review process for screening requests from our development organizations for the use of open source. However, we~~ cannot be sure that all open source, including open source that incorporates or relies on ~~generative~~ **Gen** AI, is submitted for approval prior to use in our products. In addition, many of the risks associated with usage of open source, including open source that incorporates or relies on ~~generative~~ **Gen** AI, may not or cannot be eliminated and could, if not properly addressed, negatively affect our business **. These claims could result in litigation and if portions of our proprietary AI models or software are determined to be subject to an open- source license, or if the license terms for the open- source software that we incorporate change, we could be required to publicly release all or affected portions of our source code, purchase a costly license, cease offering the implicated products or services unless and until we can re- engineer such source code in a manner that avoids infringement, discontinue or delay the provision of our offerings if re- engineering could not be accomplished on a timely basis or change our business activities, any of which could negatively affect our business operations and potentially our intellectual property rights and help third parties, including our competitors, develop products and services that are similar to or better than ours. In addition, the re- engineering process could require us to expend significant additional research and development resources, and we may not be able to complete the re- engineering process successfully. If we were required to publicly disclose any portion of our proprietary models, it is possible we could lose the benefit of trade secret protection for our models. Use of open- source software may also present additional security risks because the public availability of such software may make it easier for hackers and other third parties to determine how to breach our website and systems that rely on open- source software. Any of these risks associated with the use of open- source software could be difficult to eliminate or manage and, if not addressed, could materially and adversely affect our business, financial condition, results of operations and cash flows** . RISKS RELATED TO OUR LIQUIDITY AND INDEBTEDNESS ~~There are risks associated with our outstanding and future indebtedness that could adversely affect our financial condition.~~ As of March ~~29~~ **28** , ~~2024~~ **2025** , we had an aggregate of $ 8, ~~716~~ **355** million of outstanding indebtedness that will mature in calendar years ~~2025~~ **2027** through ~~2030~~ **2033** , and $ 1, ~~500~~ **494** million **, net of our letters of credit,** available for borrowing under our revolving credit facility. See Note 10 of the Notes to the Consolidated Financial Statements included in this Annual Report on Form 10- K for further information on our outstanding debt. Our ability to meet expenses, comply with the covenants under our debt instruments, pay interest and repay principal for our substantial level of indebtedness depends on, among other things, our operating performance, competitive developments, and financial market conditions, all of which are significantly affected by financial, business, economic and other factors. We are not able to control many of these factors. Accordingly, our cash flow may not be sufficient to allow us to pay principal and interest on our debt, including our ~~5. 0 % Senior Notes due 2025,~~ 6. 75 % Senior Notes due 2027 ~~and~~ **,** 7. 125 % Senior Notes due 2030 **and 6. 25 % Senior Notes due 2033** (collectively, the Senior Notes), and meet our other obligations. Our level of indebtedness could have other important consequences, including the following: • We must use a substantial portion of our cash flow from operations to pay interest and principal on the Amended ~~and Restated~~ Credit Agreement, our existing Senior Notes, and other indebtedness, which reduces funds available to us for other purposes such as working capital, capital expenditures, other general corporate purposes and potential acquisitions; • We may be unable to refinance our indebtedness or to obtain additional financing for working capital, capital expenditures, acquisitions or general corporate purposes; • We have significant exposure to fluctuations in interest rates because borrowings under our senior secured credit facilities bear interest at variable rates; • Our leverage may be greater than that of some of our competitors, which may put us at a competitive disadvantage and reduce our flexibility in responding to current and changing industry and financial market conditions; • We may be more vulnerable to an economic downturn or recession and adverse developments in our business; • We may be unable to comply with financial and other covenants in our debt agreements, which could result in an event of default that, if not cured or waived, may result in acceleration of certain of our debt and would have an adverse effect on our business and prospects and could force us into bankruptcy or liquidation; and • Changes by any rating agency to our outlook or credit rating could negatively affect the value of our debt and / or our common stock, adversely affect our access to debt markets and increase the interest we pay on outstanding or future debt. There can be no assurance that we will be able to manage any of these risks successfully. In addition, we conduct a significant portion of our operations through our subsidiaries. Accordingly, repayment of our indebtedness will be dependent in part on the generation of cash flow by our subsidiaries and their respective abilities to make such cash available to us by dividend, debt repayment or otherwise, which may not always be possible. If we do not receive distributions from our subsidiaries, we may be unable to make the required principal and interest payments on our indebtedness. Our Amended ~~and Restated Credit Agreement imposes operating and financial restrictions on us. Our Amended and Restated~~ Credit Agreement contains covenants that limit our ability and the ability of our restricted subsidiaries to: • Incur additional debt; • Create liens on certain assets to secure debt; • Enter into certain sale and leaseback transactions; • Pay dividends on or make other distributions in respect of our capital stock or make other restricted payments; and • Consolidate, merge, sell or otherwise dispose of all or substantially all of our assets. These covenants may adversely affect our ability to finance our operations, meet or otherwise address our capital needs, pursue business opportunities, react to market conditions or may otherwise restrict activities or business plans. A breach of any of these covenants could result in a default. If a default occurs, the relevant lenders could declare the indebtedness, together with accrued interest and other fees, to be immediately due and payable and, to the extent such indebtedness is secured, proceed against any collateral securing that indebtedness. ~~The failure of financial institutions or transactional counterparties could adversely affect our current and projected business operations and our financial condition and result of operations.~~ We regularly maintain cash balances with other financial institutions in excess of the FDIC insurance limit. A failure of a depository institution to return deposits could result in a loss or impact access to our invested cash or cash equivalents and could adversely impact our operating liquidity and financial performance. Additionally, future adverse developments with respect to specific financial institutions or the broader financial services industry may lead to market- wide

liquidity shortages, impair the ability of companies to access near- term working capital needs, and create additional market and economic uncertainty. Our general business strategy, including our ability to access existing debt under the terms of our Amended ~~and Restated~~ Credit Agreement may be adversely affected by any such economic downturn, liquidity shortages, volatile business environment or continued unpredictable and unstable market conditions. If the current equity and credit markets deteriorate, or if adverse developments are experienced by financial institutions, it may cause short- term liquidity risk and also make any necessary debt or equity financing more difficult, more costly, more onerous with respect to financial and operating covenants and more dilutive. Failure to secure any necessary financing in a timely manner and on favorable terms could have a material adverse effect on our operations, growth strategy, financial performance and stock price and could require us to alter our operating plans. ~~Hedging~~ **We rely on a variety of funding sources to support** ~~or~~ **our business model. If our existing funding arrangements are not renewed or replaced or our existing funding sources are unwilling or unable to provide funding to us on terms acceptable to us, or at all, it could have a material adverse effect on our business, financial condition, results of operations and cash flows. To support the origination of loans, cash advances and** other ~~mitigation actions~~ **receivables on our platform and the growth of our business, we must maintain a variety of funding arrangements. We cannot guarantee that we will be able** to ~~mitigate against~~ **extend or replace our existing funding arrangements at maturity on reasonable terms or at all. For example, disruptions in the credit markets or other factors, such as the high inflation and** interest rate **environment** ~~exposure may adversely affect our earnings, limit our gains or result~~ in ~~losses~~ **2023** , ~~which~~ **2024, and to date in 2025,** could adversely affect **the availability, diversity, cost and terms of our funding arrangements. In addition, our funding sources may reassess their exposure to our industry or our business, including as a result of any significant underperformance of the consumer receivables facilitated through our platform or regulatory developments, in particular regarding earned wage access products, that impose significant requirements on, or increase potential risks and liabilities related to, the consumer receivables facilitated through our platform, and fail to renew or extend facilities or impose higher costs to access our funding. If our existing funding arrangements are not renewed or replaced or our existing funding sources are unwilling or unable to provide funding on terms acceptable to us, or at all, we would need to secure additional sources of funding or reduce our operations significantly, which could have a material adverse effect on our business, financial condition, results of operations and** cash **flows** ~~available for distributions~~ . We have previously and may in the future enter into interest rate swap agreements or pursue other interest rate hedging strategies. In March 2023, we entered into interest rate swap agreements to mitigate risks associated with the variable interest rate of our Term A Facility. These pay- fixed, receive- floating rate interest rate swaps have the economic effect of hedging the variability of forecasted interest payments until their maturity on March 31, 2026. Pursuant to the agreements, we have effectively converted $ 1 billion of our variable rate borrowings under Term A Facility to fixed rates, with $ 500 million at a fixed rate of 3. 762 % and $ 500 million at a fixed rate of 3. 550 %. The objective of our interest rate swaps, all of which are designated as cash flow hedges, is to manage the variability of future cash interest expense. Our future hedging activity will vary in scope based on the level of interest rates, the type and expected duration of portfolio investments held, and other changing market conditions. Our current and future interest rate hedging may fail to protect or could adversely affect us because, among other things: • Interest rate hedging can be expensive, particularly during periods of rising and volatile interest rates; • Available interest rate hedging may not correspond directly with the interest rate risk for which protection is sought; • The duration of the hedge may not match the duration of the related liability or asset; • The credit quality of the party owing money on the hedge may be downgraded to such an extent that it impairs our ability to sell or assign our side of the hedging transaction; • The party owing money in the hedging transaction may default on its obligation to pay; and • We may purchase a hedge that turns out not to be necessary (i. e., a hedge that is out of the money). Any hedging activity we engage in may adversely affect our earnings, which could adversely affect cash available for distributions. Unanticipated changes in interest rates may result in poorer overall investment performance than if we had not engaged in any such hedging transactions. In addition, the degree of correlation between price movements of the instruments used in a hedging strategy and price movements in the portfolio positions being hedged or liabilities being hedged may vary materially. Moreover, for a variety of reasons, we may not seek to establish a perfect correlation between such hedging instruments and the portfolio holdings being hedged. Any such imperfect correlation may prevent us from achieving the intended hedge and expose us to risk of loss. GENERAL RISKS **Adverse macroeconomic conditions and** ~~Government~~ **government** efforts to combat inflation, along with other interest rate pressures arising from an inflationary economic environment, have led to and may continue to lead to higher financing costs **and may particularly have negative effects on the consumer finance industry and our MoneyLion business** . We operate globally and as a result our business and revenues are impacted by global macroeconomic conditions. ~~Inflation has risen on a global~~ **Global** ~~basis, including in the United States, and government entities have taken various actions to combat inflation, such as raising interest rate benchmarks. While the Federal Reserve has recently held inflation rates steady, global~~ inflation remains high and government entities may continue their efforts, or implement additional efforts, to combat inflation, which may include continuing to raise interest rate benchmarks or maintaining interest rate benchmarks at elevated levels. Such government efforts, along with other interest rate pressures arising from an inflationary economic environment, ~~have~~ **could** ~~led~~ **lead** to **us to incur even** higher **interest rates and** financing costs **and have material adverse effect on our business, operating results, profitability and cash flows** . For example, recent elevated interest rates have resulted in an increase in our cost of debt. These government actions and global macroeconomic conditions **, including trade wars, fluctuating tariff rates, and risks of recession,** have had and may continue to have a material adverse effect on our business, financial condition ~~and~~ **,** results of operations **and cash flows** . ~~Fluctuations in~~ **In addition, adverse macroeconomic conditions may cause our MoneyLion Product Partners to reduce their marketing spend** ~~our~~ **or** ~~quarterly~~ **advertising on our platform, which could have a material adverse effect on our business,** financial **condition,** results **of operations and cash flows. Uncertainty and negative trends in general economic conditions, including significant tightening of credit markets, historically** have **created a difficult operating**

environment for the consumer finance industry. The timing and extent of an economic downturn may also require us to change, postpone or cancel our strategic initiatives or growth plans to pursue shorter- term sustainability. The longer and more severe an economic downturn, the greater the potential adverse impact on us, which could be material. Many new customers on our MoneyLion platform have limited or no credit history and limited financial resources. Accordingly, such customers have historically been, and may in the future become, disproportionately affected **by adverse macroeconomic conditions, potentially impacting our ability to make accurate assessments or decisions about our customers' ability to pay for loans, repay cash advances or pay for other products and services MoneyLion provides. In addition, sustained high levels of unemployment may increase the non- repayment rate on our MoneyLion loans and cash advance products, increase the rate of customers declaring bankruptcy or decrease our customers' use of our investment and other products and services. If we are unable to adjust our business operations to account for rises in unemployment, or if our platform is unable to more successfully predict the creditworthiness of potential borrowers compared to other lenders,** ~~the~~ **then** ~~trading price of~~ our ~~stock in the past~~ **business, financial condition, results of operations** and **cash flows** could **be adversely affected. Increased interest rates, which often lead to higher payment obligations, may adversely impact the spending level of consumers and their willingness and ability to borrow money, resulting in decreased borrower demand for our lending products or those provided by our Product Partners. Any sustained decline in demand for loans, cash advances or other products and services we offer, or any increase in delinquencies or defaults that result from economic downturns, may harm our ability to maintain robust volumes for our business, which would adversely** affect **our financial condition, results of operations and cash flows. Furthermore, inflationary and** ~~the~~ **other** ~~trading price~~ **economic pressure resulting in the inability** of **a borrower to repay a loan could translate into increased loan delinquencies, defaults, bankruptcies** ~~our~~ **or** ~~stock in the future~~ **foreclosures and charge- offs and decreased recoveries, all of which could negatively affect our business, financial condition, results of operations and cash flows** . Our quarterly financial results have fluctuated in the past and are likely to vary in the future due to a number of factors, many of which are outside of our control. If our quarterly financial results or our predictions of future financial results fail to meet our expectations or the expectations of securities analysts and investors, the trading price of our outstanding securities could be negatively affected. Volatility in our quarterly financial results may make it more difficult for us to raise capital in the future or pursue acquisitions. Factors associated with our industry, the operation of our business, and the markets for our solutions may cause our quarterly financial results to fluctuate, including but not limited to: • Fluctuations in demand for our solutions; • Disruptions in our business operations or target markets caused by, among other things, terrorism or other intentional acts, outbreaks of disease, or earthquakes, floods or other natural disasters; • Entry of new competition into our markets; • Technological changes in our markets; • Our ability to achieve targeted operating income and margins and revenues; • Competitive pricing pressure or free offerings that compete with one or more of our solutions; • Our ability to timely complete the release of new or enhanced versions of our solutions; • The amount and timing of commencement and termination of major marketing campaigns; • The number, severity and timing of threat outbreaks and cyber security incidents; • Loss of customers or strategic partners or the inability to acquire new customers or cross- sell our solutions; • Changes in the mix or type of solutions and subscriptions sold and changes in consumer retention rates; • The rate of adoption of new technologies and new releases of operating systems, and new business processes; • Consumer confidence and spending changes; • The outcome or impact of litigation, claims, disputes, regulatory inquiries or investigations; • The impact of acquisitions (and our ability to achieve expected synergies or attendant cost savings), divestitures, restructurings, share repurchase, financings, debt repayments, equity investments and other investment activities; • Changes in U. S. and worldwide economic conditions, such as economic recessions, the impact of inflation, fluctuations in foreign currency exchange rates including the weakening of foreign currencies relative to USD, which has and may in the future negatively affect our revenue expressed in USD, changes in interest rates, geopolitical conflicts ~~,~~ and other global macroeconomic factors on our operations and financial performance; • The publication of unfavorable or inaccurate research reports about our business by cybersecurity industry analysts; • The success of our ~~ESG~~ **sustainability** initiatives; • Changes in tax laws, rules and regulations; • Changes in tax rates, benefits and expenses; and • Changes in consumer protection laws and regulations. Any of the foregoing factors could cause the trading price of our outstanding securities to fluctuate significantly. **In connection with the MoneyLion acquisition, we entered into a Contingent Value Rights Agreement dated April 17, 2025 (the " CVR Agreement ") governing the terms of the CVRs. Each CVR entitles its holder to receive $ 23. 00 shares of common stock, par value $ 0. 01 per share, of Gen Digital if, on any date prior to the second anniversary of the closing, the Average VWAP (as defined in the CVR Agreement) of our common stock for 30 consecutive trading days is equal to or greater than $ 37. 50 (subject to certain adjustments) or we undergo a change of control. To the extent we are required to issue shares to the CVR holders under the CVR Agreement, our stockholders may be diluted. For additional information on our obligations under the CVR Agreement, refer to Exhibit 10. 42 to this Annual Report on Form 10- K for a copy of the CVR Agreement.** ~~RISK~~ **RISKS** RELATED TO TAXES Changes to our effective tax rate, including through the adoption of new tax legislation or exposure to additional income tax liabilities, could increase our income tax expense and reduce (increase) our net income (loss), cash flows and working capital. In addition, audits by tax authorities could result in additional tax payments for prior periods. We are a multinational company dual headquartered in the U. S. and the Czech Republic, with our principal executive offices in Tempe, Arizona. As such, we are subject to tax in multiple U. S. and international tax jurisdictions. Our effective tax rate could be adversely affected by several factors, many of which are outside of our control, including: • Changes to the U. S. federal income tax laws, including the potential for federal tax law changes put forward by Congress and the current administration including potentially increased corporate tax rates, new minimum taxes and other changes to the way that our ~~US~~ **U. S.** tax liability has been calculated following the 2017 Tax Cuts and Jobs Act. **Such potential changes** ~~Certain of these proposals~~ could have significant retroactive adjustments adding cash tax payments / liabilities if adopted; • Changes to other tax laws, regulations, and interpretations in multiple jurisdictions in which we operate **.**

The ~~, including actions resulting from the~~ Organisation for Economic Co- operation and Development ~~' s~~ (**“** OECD **”**) ~~base erosion and profit~~ **has proposed certain tax reforms, which, among other things, (1)** ~~shifting~~ --- **shift** ~~project including recent proposals for~~ **taxing rights to the jurisdiction of the consumer (“ Pillar One ”) and (2) establish** a global minimum tax **for** ~~rate, proposed actions by international bodies such as digital services taxation, as well as the requirements of certain tax rulings. In October 2021, the OECD / G20 inclusive framework on Base Erosion and Profit Shifting (the Inclusive Framework) published a statement updating and finalizing the key components of a two- pillar plan on global tax reform which has now been agreed upon by the majority of OECD members. OECD and many countries have proposed to reallocate a portion of profits of large~~ multinational **companies** ~~enterprises (MNE) with an annual global turnover exceeding € 20 billion to markets where sales arise (Pillar One), as well as enact a global minimum tax rate~~ of 15 % ~~for MNE with an annual global turnover exceeding € 750 million~~ (**“** Pillar Two **”**) ~~. On December 12, 2022, the European Union reached an agreement to implement the Pillar Two Directive of the OECD' s reform of international taxation at the European Union level. The agreement affirms that all Member States must transpose the Directive by December 31, 2023. The rules will therefore first be applicable for fiscal years starting on or after December 31, 2023~~ . Ireland, Czech Republic and certain jurisdictions in which we operate have enacted legislation to implement Pillar Two and other countries are actively considering changes to their tax laws to adopt certain parts of the OECD' s proposals. The enactment of Pillar Two legislation is not expected to have a material adverse effect on our effective tax rate and Consolidated Financial Statements in the near term **. Additionally, several countries have proposed or adopted digital services taxes on revenue earned by multinational companies from the provision of certain digital services, regardless of physical presence** . We will continue to monitor and reflect the impact of such legislative changes in future financial statements as appropriate; • Changes in the relative proportions of revenues and income before taxes in the various jurisdictions in which we operate that have differing statutory tax rates; • Changes in the valuation of deferred tax assets and liabilities and the discovery of new information in the course of our tax return preparation process; • The ultimate determination of our taxes owed in any of these jurisdictions is for an amount in excess of the tax provision we have recorded or reserved for; • The tax effects of, and tax planning and changes in tax rates related to significant infrequently occurring events (including acquisitions, divestitures and restructurings) that may cause fluctuations between reporting periods; • Tax assessments, or any related tax interest or penalties, that could significantly affect our income tax expense for the period in which the settlements take place; and • Taxes arising in connection to changes in our workforce, corporate and legal entity structure or operations as they relate to tax incentives and tax rates. From time to time, we receive notices that a tax authority in a particular jurisdiction believes that we owe a greater amount of tax than we have reported to such authority and we are consequently subject to tax audits. These audits can involve complex issues, which may require an extended period of time to resolve and can be highly judgmental. Additionally, our ability to recognize the financial statement benefit of tax refund claims is subject to change based on a number of factors, including but not limited to, changes in facts and circumstances, changes in tax laws, correspondence with tax authorities, and the results of tax audits and related proceedings, which may take several years or more to resolve. ~~If tax authorities disagree with certain tax reporting positions taken by us, as a result, they assess additional taxes against us. We are regularly engaged in discussions and sometimes disputes with these tax authorities.~~ We ultimately sometimes have to engage in litigation to achieve the results reflected in our tax estimates, and such litigation can be time consuming and expensive ~~. We regularly assess the likely outcomes of any audits in order to determine the appropriateness of our tax provision~~ . If the ultimate determination of our taxes owed in any of these jurisdictions is for an amount in excess of the tax provision we have recorded or reserved for, our operating results, cash flows, and financial condition could be materially and adversely affected. Our corporate and legal entity structure and intercompany arrangements are subject to the tax laws of various jurisdictions, and we could be obligated to pay additional taxes, which would harm our results of operations. We generally conduct our international operations through wholly- owned subsidiaries and are or may be required to report our taxable income in various jurisdictions worldwide based upon our business operations in those jurisdictions. Our intercompany relationships are subject to complex transfer pricing regulations administered by taxing authorities in various jurisdictions. The amount of taxes we pay in different jurisdictions may depend on a variety of factors including the application of the tax laws of those various jurisdictions (including the U. S.) to our international business activities, changes in tax rates, new or revised tax laws or interpretations of existing tax laws and policies, and our ability to operate our business in a manner consistent with our corporate structure and intercompany arrangements. The relevant taxing authorities have in the past and may in the future disagree with our determinations as to the income and expenses attributable to specific jurisdictions. If such a disagreement were to occur, and our position was not sustained, we could be required to pay additional taxes, interest and penalties, which could result in one- time tax charges, higher effective tax rates, reduced cash flows and lower overall profitability of our operations. ~~Any changes or interpretations to existing accounting pronouncements or taxation rules or practices may cause fluctuations in our reported results of operations or affect how we conduct our business. A change in accounting pronouncements or taxation rules or practices could have a significant effect on our reported results and may affect our reporting of transactions completed before the change is effective. New accounting pronouncements, taxation rules and varying interpretations of accounting pronouncements or taxation rules have occurred in the past and may occur in the future. We could be required to modify a current tax or accounting position as a result of any such change, and this could adversely affect our reported financial results and could change the way we conduct our business.~~