Risk Factors Comparison 2024-03-27 to 2023-03-29 Form: 10-K

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

Investing in our Class A common stock involves a high degree of risk. You should carefully consider the risks and uncertainties described below, together with all of the other information in this Annual Report on Form 10- K, including the section titled " Management' s Discussion and Analysis of Financial Condition and Results of Operations, " and our consolidated financial statements and the accompanying notes included before making a decision to invest in our Class A common stock. Our business, financial condition, operating results, or prospects could also be adversely affected by risks and uncertainties that are not presently known to us or that we currently believe are not material. If any of the risks actually occur, our business, financial condition, operating results, and prospects could be adversely affected. In that event, the market price of our Class A common stock could decline, and you could lose all or part of your investment. Summary Risk Factors Our business is subject to numerous risks and uncertainties, including those risks more fully described below. These risks include, among others, the following, which we consider our most material risks: Risks Related to Our Business and Industry ~~•~~ • We have a limited operating history, which makes it difficult to evaluate our current business and future prospects and increases the risks associated with your investment. ~~•~~ • We have a history of losses, anticipate increases in our operating expenses in the future, and may not achieve or sustain profitability. If we cannot achieve and sustain profitability, our business, operating results, and financial condition will be adversely affected. ~~•~~ • We face intense competition and could lose market share to our competitors, which would adversely affect our business, operating results, and financial condition. ~~•~~ • Our operating results may fluctuate significantly, which could make our future results difficult to predict and could cause our operating results to fall below expectations. ~~•~~ • Adverse **global** ~~economic~~ **macroeconomic** conditions or reduced information technology spending could adversely affect our business, operating results **,** and financial condition. ~~•~~ • A network or data security incident against us, whether actual, alleged, or perceived, would harm our reputation, create liability, and regulatory exposure, and adversely affect our business, operating results, and financial condition. ~~•~~ • Defects, errors, or vulnerabilities in our platform, the failure of our platform to block malware or prevent a security breach, misuse of our platform, or risks of product liability claims would harm our reputation and adversely affect our business, operating results, and financial condition. ~~•~~ • Existing and future acquisitions, strategic investments, partnerships **,** or alliances could be difficult to identify and integrate, divert the attention of key management personnel, disrupt our business, dilute stockholder value and adversely affect our business, operating results, and financial condition. ~~•~~ • If we are unable to retain our customers, renew and expand our relationships with them, and add new customers, we may not be able to sustain revenue growth, and we may not achieve or maintain profitability in the future. • If our platform is not effectively interoperated within our customers' IT infrastructure, deployments could be delayed or canceled, which would adversely affect our business, operating results, and financial condition. • Disruptions or other business interruptions that affect the availability of our platform could adversely affect our customer relationships and overall business. • We may not be able to timely and cost- effectively scale and adapt our existing technology to meet our customers' performance and other requirements. • If we are unable to maintain successful relationships with our channel partners and alliance partners, or if our channel partners or alliance partners fail to perform, our ability to market, sell and distribute our platform will be limited, and our business, operating results, and financial condition will be harmed. Risks Related to Regulatory Matters • If we fail to adequately protect personal information or other information we collect, process, share, or maintain under applicable laws, our business, operating results, and financial condition could be adversely affected. Risks Related to Our People • We rely on our management team and other key employees and will need additional personnel to grow our business, and the loss of one or more key employees or our inability to hire, integrate, train, manage, retain, and motivate qualified personnel, including members of our board of directors, could harm our business. Risks Related to ~~our~~ **Our** Intellectual Property • Our proprietary rights may be difficult to enforce, which could enable others to copy or use aspects of our platform without compensating us. • Third parties have claimed and may claim in the future that our platform infringes their intellectual property rights **,** and this may create liability for us or otherwise adversely affect our business, operating results **,** and financial condition. Risks Related to Ownership of Our Class A Common Stock • The market price of our Class A common stock may be volatile, and you could lose all or part of your investment. • The dual class structure of our common stock has the effect of concentrating voting control with certain stockholders who held our capital stock prior to the completion of our IPO, including our directors, executive officers, and other beneficial owners who hold in the aggregate approximately ~~85~~ **72** % of the voting power of our capital stock, which will limit or preclude your ability to influence corporate matters, including the election of directors and the approval of any change of control transaction ~~. General Risk Factors • Adverse economic conditions or reduced information technology spending could adversely affect our business, operating results, and financial condition~~ . We were founded in January 2013 and released our first endpoint security solution in February 2015. Our limited operating history and financial data may make it difficult to evaluate our current business, future prospects and other trends. We have encountered, and will continue to encounter, risks and uncertainties frequently experienced by growing companies in rapidly changing industries and sectors, such as the risks and uncertainties described herein. Any predictions about our future revenue and expenses may not be as accurate as they would be if we had a longer operating history or operated in a more predictable or established market. If our assumptions regarding these risks and uncertainties are incorrect or change due to fluctuations in our markets or otherwise, or if we do not address these risks successfully, our operating and financial results could differ materially from our expectations **,** and our business and operating results would be adversely affected. We cannot assure you that we will be successful in addressing these and other challenges we may face in the future. **The risks associated with having a limited operating history may be**

exacerbated by current global macroeconomic conditions. We have incurred net losses in all periods since our inception, and we may not achieve or maintain profitability in the future. We experienced a net loss of $ ~~378~~ **338** . 7 million and $ ~~271~~ **378** . ~~1~~ **7** million for the fiscal years ended January 31, **2024 and** 2023 ~~and 2022~~ , respectively. As of January 31, ~~2023~~ **2024** , we had an accumulated deficit of $ 1 ~~, 000~~ . ~~4~~ **3** ~~million~~ **billion** . While we have **historically** experienced significant growth in revenue ~~in recent periods~~ , we cannot predict when or whether we will reach or maintain profitability. We also expect our operating expenses to increase in the future as we continue to invest for our future growth, including expanding our research and development function to drive further development of our platform, expanding our sales and marketing activities, developing the functionality to expand into adjacent markets, and reaching customers in new geographic locations, which will negatively affect our operating results if our total revenue does not increase. In addition to the anticipated costs to grow our business, we have incurred and expect to continue to incur significant additional legal, accounting, and other expenses as a public company **, particularly now that we are no longer an emerging growth company** . Our revenue growth is expected to slow ~~or decline~~ **as we grow** and our revenue may decline for a number of other reasons, including reduced demand for our platform, increased competition, a decrease in the growth or reduction in size of our overall market, or if we cannot capitalize on growth opportunities, including acquisitions, new products, services, and feature releases. **While we consistently evaluate opportunities to reduce our operating costs and optimize efficiencies, including, for example, our restructuring plan in June 2023, we cannot guarantee that these efforts will be successful or that we will not re- accelerate operating expenditures in the future in order to capitalize on growth opportunities.** If we fail to increase our revenue to offset increases in our operating expenses ~~,~~ or manage our costs as we invest in our business, we may not achieve or sustain profitability. The market for cybersecurity products and services is intensely competitive, fragmented and is rapidly evolving, characterized by changes in technology, customer requirements, industry standards, increasingly sophisticated attackers **,** and ~~by~~ frequent introductions of new or improved products and services. We expect to continue to face intense competition from current competitors, as well as from new entrants into the market **, as our competitors complete strategic acquisitions or form cooperative relationships and / or customer requirements evolve** . If we are unable to anticipate or react to these challenges, our competitive position could weaken, and we would experience a decline in revenue or reduced revenue growth, and loss of market share that would adversely affect our business, operating results, and financial condition. ~~Our~~ **For a description of our** competitors ~~and potential competitors include the following: • endpoint security providers~~ , **see the section titled " Business — Competition** ~~such as CrowdStrike and VMware; • legacy anti- virus providers such as Trellix, Symantec, and Microsoft; and • providers of general network security products and services who offer a broad portfolio of solutions, such as Palo Alto Networks~~ . **"** Our ability to compete effectively depends upon numerous factors, many of which are beyond our control, including, but not limited to: • our ability to attract and retain new customers, expand our platform or sell additional products and services to our existing customers ~~;~~ **;** • our ability to attract, train, retain, and motivate talented employees; • **our ability to successfully incorporate new technologies into our platform, including AI; •** the budgeting cycles, seasonal buying patterns, and purchasing practices of our customers, including any slowdown in technology spending due to **US** ~~U. S.~~ and **general** global ~~macro-~~ **macroeconomic conditions; • general global macroeconomic and political conditions, both domestically and in our foreign markets that could impact some or all regions where we operate, including global** economic ~~issues~~ **slowdowns** , ~~including~~ **actual or perceived** global banking and finance related issues, ~~rising~~ **increased risk of inflation, potential uncertainty with respect to the federal debt ceiling and budget and potential government shutdowns related thereto,** interest ~~rates~~ **rate volatility** ~~, overall market downturns, inflation~~ , supply chain disruptions, **labor shortages, and potential global recession; •** the ~~COVID~~ **impact of natural or man** - ~~19 pandemic~~ **made global events on** ~~or~~ **our** ~~otherwise~~ **business, including wars and other armed conflict, such as the conflicts in the Middle East, Ukraine and the tensions between China and Taiwan** ; • changes in customer, distributor or reseller requirements or market needs ; • price competition; • the timing and success of new product and service introductions by us or our competitors or any other change in the competitive landscape of our industry, including consolidation among our competitors or customers and strategic partnerships entered into by and between our competitors ; • changes in our mix of products, subscriptions and services sold, including changes in the average contract length for subscriptions and support ; • our ability to successfully and continuously expand our business domestically and internationally; • changes in the growth rate of endpoint security, cloud security **,** and overall cybersecurity product platform and services sectors; • deferral of orders from customers in anticipation of new or enhanced products and services announced by us or our competitors ; • significant security breaches of, technical difficulties with **,** or interruptions to ~~,~~ the use of our platform; • the timing and costs related to the development or acquisition of technologies ~~or ,~~ businesses **,** or strategic partnerships ; • our ability to execute, complete **,** or **efficiently** integrate ~~efficiently~~ any acquisitions that we may undertake ; • increased expenses, unforeseen liabilities, or write- downs and any impact on our operating results from any acquisitions we consummate ; • our ability to increase the size and productivity of our distribution channels ; • decisions by potential customers to purchase security solutions from larger, more established security vendors or from their primary network equipment vendors ; • timing of revenue recognition and revenue deferrals ; • insolvency or credit difficulties confronting our customers, which could increase due to **US** ~~U. S.~~ and global ~~macro- economic~~ **macroeconomic** issues, including **actual or perceived** global banking and finance related issues, inflation, ~~rising~~ interest ~~rates~~ - **rate volatility** , **and** market downturns ~~and the effects of the COVID- 19 pandemic~~ , which would adversely affect their ability to purchase or pay for our platform, products, and services in a timely manner or at all; • the cost and potential outcomes of litigation or other proceedings, which could have a material adverse effect on our business ; • future accounting pronouncements or changes in our accounting policies ; **and** • increases or decreases in our expenses caused by fluctuations in foreign currency exchange rates ~~; and • general macroeconomic conditions, both domestically and in our foreign markets that could impact some or all regions where we operate, including global economic slowdowns, global banking and finance related issues, increased risk of inflation, rising interest rates, labor shortages and potential global recession~~ . Many of our competitors have greater financial, technical,

marketing, sales, and other resources, greater name recognition, longer operating histories, and a larger base of customers than we do. Our competitors may be able to devote greater resources to the development, promotion and sale of their products and services than we can, and they may offer lower pricing than we do or bundle certain competing products and services at lower prices. Our competitors may also have greater resources for research and development of new technologies, customer support and to pursue acquisitions, or they may have other financial, technical, or other resource advantages. Our larger competitors have substantially broader and more diverse product and service offerings and more mature distribution and go- to- market strategies, which allows them to leverage their existing customer and distributor relationships to gain business in a manner that discourages potential customers from purchasing our platform. Conditions in our market could change rapidly and significantly as a result of technological advancements, including but not limited to increased advancements and proliferation in the use of open artificial intelligence applications, partnering or acquisitions by our competitors or continuing market consolidation. Some of our competitors have recently made or could make acquisitions of businesses or have established cooperative relationships that may allow them to offer more directly competitive and comprehensive products and services than were previously offered and adapt more quickly to new technologies and customer needs. These competitive pressures in our market or our failure to compete effectively may result in price reductions, fewer orders, reduced revenue and gross margin, increased net losses **,** and loss of market share. Even if there is significant demand for endpoint and cloud security solutions like ours, if our competitors include functionality that is, or is perceived to be, equivalent to or better than ours in legacy products that are already generally accepted as necessary components of an organization' s IT security architecture, we will have difficulty increasing the market penetration of our platform. Furthermore, even if the functionality offered by other cybersecurity providers is different and more limited than the functionality of our platform, organizations may elect to accept such limited functionality in lieu of purchasing products and services from additional vendors like us. If we are unable to compete successfully, or if competing successfully requires us to take aggressive action with respect to pricing or other actions, our business, financial condition **,** and operating results would be adversely affected. Our operating results have varied significantly from period to period in the past, and we expect that our operating results will continue to vary significantly in the future such that period- to- period comparisons of our operating results may not be meaningful. This could adversely affect our business, operating results, and financial condition. Accordingly, our financial results in any one quarter should not be relied upon as indicative of future performance. Fluctuations in quarterly results may negatively impact the trading price of our Class A common stock. Our quarterly financial results may fluctuate as a result of a number of factors, many of which are outside of our control and may be difficult to predict, including, without limitation: • general **global** ~~economic,~~ macroeconomic and political conditions, both ~~domestic~~ **domestically** and in our foreign markets ~~,~~ that could impact some or all regions where we operate, including ~~any~~ global economic ~~slowdown~~ **slowdowns** , **actual or perceived** global banking and finance related issues, increased risk of inflation, ~~rising~~ **potential uncertainty with respect to the federal debt ceiling and budget and potential government shutdowns related thereto,** interest ~~rates~~ **rate volatility, supply chain disruptions** , labor shortages and potential global recession **; • the impact of natural or man- made global events on our business** , **including** ~~war~~ **wars and other** ~~, terrorism or~~ armed conflict, ~~including Russia' s invasion of~~ **such as the conflicts in the Middle East,** Ukraine **and tensions between China and Taiwan** ~~, or instability in the global system~~ ; • our ability to attract new and retain existing customers or sell additional features to existing customers; • the budgeting cycles, seasonal buying patterns, and purchasing practices of customers; • the timing and length of our sales cycles; • changes in customer or channel partner requirements or market needs; • changes in the growth rate of the cybersecurity market generally and market for endpoint security; • the timing and success of new product and service introductions by us **, including PinnacleOne, our strategic risk analysis and advisory group, and Singularity Data Lake, our live enterprise data platform for data queries, analytics, insights, and retention,** or our competitors or any other competitive developments, including consolidation among our customers or competitors; • the level of awareness of cybersecurity threats, particularly advanced cyberattacks, and the market adoption of our platform; • our ability to successfully expand our business domestically and internationally; • decisions by organizations to purchase security solutions from larger, more established security vendors or from their primary IT equipment vendors; • changes in our pricing policies or those of our competitors; • any disruption in our relationship with ISVs, channel partners, MSPs, MSSPs, MDRs, OEMs **,** and IR firms; • insolvency or credit difficulties confronting our customers, affecting their ability to purchase or pay for our solution **; • significant security breaches of, technical difficulties with, or interruptions to, the use of our platform or other cybersecurity incidents** ; • extraordinary expenses such as litigation or other dispute- related settlement payments or outcomes, taxes, regulatory fines or penalties; • ~~the impact of the COVID- 19 pandemic on our operations, financial results, and liquidity and capital resources, including on customers, sales, expenses, and employees; •~~ future accounting pronouncements or changes in our accounting policies or practices; • negative media coverage or publicity; • the amount and timing of operating costs and capital expenditures related to the expansion of our business; and ~~• increases or decreases in our expenses caused by fluctuations in foreign currency exchange rates.~~ In addition, we experience seasonal fluctuations in our financial results as we typically receive a higher percentage of our annual orders from new customers, as well as renewal orders from existing customers, in our fourth fiscal quarter as compared to other quarters due to the annual budget approval process of many of our customers. Any of the above factors, individually or in the aggregate, may result in significant fluctuations in our financial and other operating results from period to period. As a result of this variability, our historical operating results should not be relied upon as an indication of future performance. Moreover, this variability and unpredictability could result in our failure to meet our operating plan or the expectations of investors or analysts for any period. If we fail to meet such expectations for the reasons described above or other reasons, our stock price could fall substantially, and we could face costly lawsuits, including securities class action ~~suits~~ **lawsuits** . Our **business depends on the overall demand for information technology and on the economic health of our current and prospective customers. In addition, the purchase of our** platform ~~represents~~ **is often discretionary and may involve** a ~~involve a~~ significant commitment of capital and other resources.Weak global and regional economic conditions,including **US**

~~U.S.~~ and global macro- economic issues, ~~including~~ **actual or perceived** global banking and finance related issues,labor shortages,supply chain disruptions,rising interest rates and inflation,spending environments,geopolitical instability,warfare and uncertainty,weak economic conditions in certain regions or a reduction in information technology spending regardless of macro-economic conditions,including the effects of the **conflicts in** ~~COVID- 19 pandemic and~~ the ~~war in~~ **Middle East,** Ukraine,and ~~proposed~~ **tensions between China and Taiwan and** judicial reform in Israel,could adversely affect our business,operating results,and financial condition,including resulting in longer sales cycles,a negative impact on our ability to attract and retain new ~~approach to endpoint protection~~ **customers or expand our platform or sell additional products** and **services to our existing customers** , ~~therefore~~ **lower prices for our platform** , ~~including resulting in longer sales cycles,a negative impact on our ability to attract and retain new customers or expand our platform or sell additional products and services to our existing customers,lower prices for our platform,~~ higher default rates among our channel partners,reduced sales to new or existing customers and slower or declining growth.For example,as a result of current uncertainty in macroeconomic conditions **and related** ~~,we have recently observed a lengthening of the sales cycle for some prospective customers that we attribute to~~ higher cost ~~–~~consciousness around IT budgets **,we have recently experienced certain impacts on our business,including a decline in usage and consumption patterns from certain customers,especially larger enterprise customers,longer sales cycles,and deal downsizing by new customers and of renewals by existing customers,especially larger enterprises** .We expect the **global** macroeconomic conditions impacting demand to persist in the near ~~–~~term.Deterioration in economic conditions in any of the countries in which we do business could also cause slower or impaired collections on accounts receivable,which may adversely impact our liquidity and financial condition.Moreover,the **US** ~~U.S.~~ capital markets have experienced and continue to experience extreme volatility and disruption.Inflation rates in the **US** ~~U.S.~~ significantly increased in **2021 and** 2022 **,** resulting in federal action to increase interest rates,adversely affecting capital markets activity.Further deterioration of the macroeconomic environment and regulatory action may adversely affect our business,operating results,and financial condition. ~~Moreover~~ **We are investing in expanding our platform** , **including our cloud security products,and** it is difficult to predict adoption and demand **. We are meaningfully investing in our platform, including growing our cloud security product. For example, in November 2023, through the acquisition of KSG, we launched PinnacleOne, a strategic advisory group also operating as a think tank** for ~~our platform~~ **hire, focused on helping companies and their executives holistically understand the evolving risks of operating in the modern global business landscape through personalized access to experts' intelligence, insight, and transformative risk management strategies** . ~~Our~~ **Further, in February 2024, we acquired PingSafe, a** cloud ~~- native, artificial intelligence- enabled endpoint~~ security platform ~~represents a new approach to endpoint protection. Accordingly~~ , ~~it~~ **which we expect will enable us to couple PingSafe' s CNAPP with our cloud workload security and cloud data security capabilities. It** is difficult to predict customer adoption and demand for our platform, the size and growth rate of this market, the entry of competitive products and services or the success of existing competitive products and services. Any expansion in our market depends on a number of factors, including the cost, performance and perceived value associated with, and customer adoption of, our platform. If the market for our platform does not achieve widespread adoption or there is a reduction in demand for our software or our services caused by a lack of customer acceptance, implementation challenges for deployment, technological challenges, competing technologies and services, decreases in corporate spending, weakening economic conditions, or otherwise, it could result in reduced customer orders and decreased revenue, which would adversely affect our business operations and financial condition. Our platform interoperates with, but does not necessarily replace, other security **and log analytics** products. Businesses that use other cybersecurity products and services may be hesitant to purchase our platform if they believe their existing products and services provide a level of security that is sufficient to meet their needs. If we do not succeed in convincing customers that our platform should be an integral part of their overall approach to security, our sales will not grow as quickly as anticipated, or at all, which would have an adverse impact on our business, operating results, and financial condition. If businesses do not continue to adopt our platform for any of the reasons discussed above or for other reasons not contemplated, our sales would not grow as quickly as anticipated, or at all, and our business, operating results, and financial condition would be adversely affected. **We may not be successful in our artificial intelligence initiatives, which could adversely affect our business, reputation, or financial results. We have recently begun incorporating generative AI into our offerings, including our Purple AI solution dedicated to threat- hunting, analysis and response. As with many innovations, generative AI presents risks, challenges, and unintended consequences that could impact our successful ability to incorporate the use of generative AI in our business. For example, language models may provide flawed results or misinterpret prompts. Further, data practices by us or others that result in controversy could also impair the acceptance of AI solutions. This is turn could undermine confidence in the decisions, predictions, analyses or other content that our AI- initiatives produce. In addition, our competitors or other third parties may incorporate generative AI solutions into their products more successfully than us, and their solutions may achieve higher market acceptance than ours, which may result in us failing to recoup our investments in developing generative AI- powered offerings. We have made and expect to continue to make significant investments in our AI technology, including in our Purple AI solution. Our ability to employ AI, or the ability of our competitors to do so more successfully, may negatively impact our gross margins, impair our ability to compete effectively, result in reputational harm and have an adverse impact on our operating results. Moreover, AI may give rise to litigation risk, including potential intellectual property, privacy, or cybersecurity liability. Because AI is an emerging technology, there is not a mature body of case law construing the appropriateness of certain of its uses of data- whether through the employment of large language models or other models leveraging data found on the Internet- and the evolution of this law may limit our ability to exploit artificial intelligence tools, or expose us to litigation. Further, AI presents emerging ethical issues and if our use of AI algorithms draws controversy due to their perceived or actual impact on society, we may experience brand or reputational harm, competitive harm or legal liability. In addition, given the complex nature of AI technology, we face an evolving**

regulatory landscape. For example, in October 2023, President Biden issued an Executive Order that establishes new standards for, among other things, AI safety, security, and privacy. Moreover, we are subject to significant competition from other companies, some of which have longer operating histories and significantly greater financial, technical, marketing, distribution, professional services, or other resources than us. Our competitors may incorporate AI into their products more quickly or more successfully than us, which could impair our ability to compete effectively and adversely affect our financial results. Any of the foregoing could adversely affect our business, reputation, or financial results. A network or data security incident against us, whether actual, alleged, or perceived, would harm our reputation, create liability and regulatory exposure, and adversely impact our business, operating results, and financial condition. Companies are subject to an increasing number and wide variety of attacks on their networks on an ongoing basis. Traditional computer " hackers, " malicious code (such as viruses and worms), phishing attempts, ransomware, account takeover, business email compromise, employee fraud, theft or misuse, denial of service attacks, and sophisticated nation- state and nation- state supported actors engage in intrusions and attacks that create risks for our internal networks and cloud deployed products and the information they store and process. Cybersecurity companies face particularly intense attack efforts, and we have faced, and will continue to face, cyber threats and attacks from a variety of sources. The research that we conduct and report may make us, or our customers, a further target for attacks of all kinds. State- supported and geopolitical- related cyberattacks may ~~increase~~ **rise** in connection with ~~Russia' s invasion of~~ **regional geopolitical conflicts such as the conflicts in the Middle East,** Ukraine and ~~any related political~~ **tensions between China and Taiwan. In addition,** ~~or~~ **our** ~~economic responses and counter- responses~~ **cybersecurity product is likely considered a valuable target for lateral attacks because of its highly privileged access** . ~~The~~ **Moreover, the ongoing** war in Ukraine and associated activities in Ukraine and Russia ~~has~~ **have** increased the risk of cyberattacks on various types of infrastructure and operations, and the **US** ~~United States~~ government has warned companies to be prepared for a significant increase in Russian cyberattacks in response to the sanctions on Russia. **There may also be increased risks of cybersecurity attacks as a result of the unfolding events in the Middle East. Additionally, bad actors are beginning to utilize AI- based tools to execute attacks, creating unprecedented cybersecurity challenges.** Although we have implemented security measures to prevent such attacks, our networks and systems may be breached due to the actions of outside parties, **human or** employee error **, insufficient cybersecurity controls** , malfeasance, a combination of these, or otherwise, and as a result, an unauthorized party may obtain access to our and / or our customers' systems, networks, or data. We may face difficulties or delays in identifying or otherwise responding to any attacks or actual or potential security breaches or threats **. These risks are exacerbated by developments in generative AI** . A breach in our data security or an attack against our platform could impact our networks or the networks and data of our customers that are secured by our platform, creating system disruptions or slowdowns and providing access to malicious parties to information stored on our networks or the networks of our customers, resulting in data being publicly disclosed, misused, altered, lost, or stolen, which could subject us to liability and adversely affect our financial condition. ~~The COVID- 19 pandemic may have~~ **If compromised, our own systems could be used to facilitate or magnify an attack. Further, the increase in remote work by companies and individuals in recent years has** generally increased the attack surface available to ~~criminals~~ **bad actors for exploitation** , **and** as **such** ~~companies and individuals work online and remotely~~ , ~~which~~ **the risk of a cybersecurity incident potentially occurring** has increased ~~the risk of a successful cyber security attack~~ . We have accordingly increased our investments in protective measures and risk mitigation strategies, but we cannot guarantee that our efforts, or the efforts of those upon whom we rely and partner with, will be successful in preventing any such information security incidents. Protecting our own assets has become more expensive from a dollar investment and time perspective **and these costs may increase as the threat landscape increases, including as a result of use by bad actors of AI** . Any actual, alleged **,** or perceived security breach in our systems or networks, or any other actual, alleged or perceived data security incident we suffer, could result in damage to our reputation, negative publicity, loss of customers and sales, loss of competitive advantages over our competitors, increased costs to remedy any problems and otherwise respond to any incident, regulatory investigations and enforcement actions **, fines and penalties** , costly litigation, and other liability. We would also be exposed to a risk of loss or litigation and potential liability under laws, regulations **,** and contracts that protect the privacy and security of personal information. For example, the California Consumer Privacy Act of 2018 (CCPA **), as amended by the California Privacy Rights Act (CPRA**), imposes a private right of action for security breaches that could lead to some form of remedy including regulatory scrutiny, fines, private right of action settlements, and other consequences. Where a security incident involves a breach of security leading to the accidental or unlawful destruction, loss, alternation, unauthorized disclosure of, or access to, personal data **from the European Economic Area (EEA) or the UK** in respect of which we are a controller or processor under the **General Data Protection Regulation (** GDPR **),** and ~~U. K.~~ **the UK General Data Protection Regulation and UK Data Protection Act 2018 (UK** GDPR ~~(as defined below~~), this could result in fines of up to € 20 million or 4 % of annual global turnover **, whichever is greater,** under the GDPR or **up to** £ 17 **. 5** million ~~and~~ **or** 4 % of ~~total~~ annual ~~revenue~~ **global turnover, whichever is greater,** in the case of the **UK** ~~U. K.~~ GDPR. We may also be required to ~~notify~~ **provide notice of** such breaches to regulators and / or individuals which may result in us incurring additional costs **, penalties, fines or litigation. Further, on July 26, 2023, the SEC adopted cybersecurity disclosure rules for public companies that require disclosure regarding cybersecurity risk management (including the board' s role in overseeing cybersecurity risks, management' s role and expertise in assessing and managing cybersecurity risks and processes for assessing, identifying and managing cybersecurity risks) in annual reports on Form 10- K. These cybersecurity disclosure rules also require the disclosure of material cybersecurity incidents by Form 8- K, within four business days of determining an incident is material. Any public disclosure relating to a material cybersecurity incident, whether as a result of the new SEC rules or otherwise, harm our reputation, result in litigation and adversely impact our business, operating results, and financial condition. In addition, certain of our customer agreements may require us to promptly report security breaches involving their data on our systems or those of subcontractors processing such data on our**

behalf. This mandatory disclosure could be costly, result in litigation, harm our reputation, erode customer trust, and require significant resources to mitigate issues stemming from actual or perceived security breaches . In addition, we may incur significant financial and operational costs to investigate, remediate, eliminate and put in place additional tools and devices designed to prevent actual or perceived security breaches and other security incidents, as well as costs to comply with any notification obligations resulting from any security incidents. Any of these negative outcomes could adversely affect the market perception of our platform and customer and investor confidence in our company, and would adversely affect our business, operating results, and financial condition. Defects, errors, or vulnerabilities in our platform, the failure of our platform to block malware or prevent a security breach, misuse of our platform, or risks of product liability claims would harm our reputation and adversely impact our business, operating results, and financial condition. Our platform and product features are multi- faceted and may be deployed with material defects, software " bugs " or errors that are not detected until after their commercial release and deployment to our customers. From time to time, certain of our customers have reported defects in our platform related to performance, scalability, and compatibility. Our platform and product features also provide our customers with the ability to customize a multitude of settings, and it is possible that a customer could misconfigure our platform or otherwise fail to configure our products in an optimal manner. Such defects and misconfigurations of our platform could cause our platform to operate at suboptimal efficacy, cause it to fail to secure customers' computing environments and detect and block threats, or temporarily interrupt ~~the functionality of~~ our customers' ~~endpoints~~ **computing environments** . We also make frequent updates to our platform, which may fail, resulting in temporary vulnerability that increases the likelihood of a material defect. In addition, because the techniques used by computer hackers to access or sabotage target computing environments change frequently and generally are not recognized until launched against a target, there is a risk that an advanced attack could emerge that our platform is unable to detect or prevent. Furthermore, as a well- known provider of security solutions, our networks, platform, products, including cloud- based technology, and customers could be targeted by attacks specifically designed to disrupt our business ~~and ,~~ harm our reputation **or use our technology to gain unauthorized access** . In addition, ~~due to the Russian invasion~~ **regional geopolitical conflicts such as** ~~there~~ -- **the** ~~could be a significant~~ **conflicts in the Middle East, Ukraine and tensions between China and Taiwan, may result in** ~~increase~~ **increased** ~~in Russian~~ cyberattacks against our customers, resulting in an increased risk of a security breach of our customers' systems. In addition, defects or errors in our platform could result in a failure to effectively update customers' cloud- based products. Our data centers and networks may experience technical failures and downtime, may fail to distribute appropriate updates, or may fail to meet the increased requirements of a growing customer base, any of which could temporarily or permanently expose our customers' computing environments, leaving their computing environments unprotected against cyber threats. Any of these situations could result in negative publicity to us, damage our reputation, and increase expenses and customer relations issues, which would adversely affect our business, financial condition, and operating results. Advances in computer capabilities, discoveries of new weaknesses and other developments with software generally used by the Internet community may increase the risk we will suffer a security breach. Furthermore, our platform may fail to detect or prevent malware, ransomware, viruses, worms or similar threats for any number of reasons, including our failure to enhance and expand our platform to reflect industry trends, new technologies and new operating environments, the complexity of the environment of our clients and the sophistication of malware, viruses and other threats. Our platform may fail to detect or prevent threats in any particular test for a number of reasons. We or our service providers may also suffer security breaches or unauthorized access to personal information, financial account information, and other confidential information due to employee error, rogue employee activity, unauthorized access by third parties acting with malicious intent or who commit an inadvertent mistake or social engineering. If we experience, or our service providers experience, any breaches of security measures or sabotage or otherwise suffer unauthorized use or disclosure of, or access to, personal information, financial account information or other confidential information, we might be required to expend significant capital and resources to address these problems. We may not be able to remedy any problems caused by hackers or other similar actors in a timely manner, or at all. To the extent potential customers, industry analysts or testing firms believe that the failure to detect or prevent any particular threat is a flaw or indicates that our platform does not provide significant value, our reputation and business would be harmed. Any real or perceived defects, errors or vulnerabilities in our platform, or any other failure of our platform to detect an advanced threat, could result in: • a loss of existing or potential customers; • delayed or lost revenue and adverse impacts to our business, operating results, and financial condition ; • a delay in attaining, or the failure to attain, market acceptance ; • the expenditure of significant financial and research and development resources in efforts to analyze, correct, eliminate, or work around errors or defects, and address and eliminate vulnerabilities ; • an increase in resources devoted to customer service and support, which could adversely affect our gross margin ; • harm to our reputation or brand ; and • claims and litigation, regulatory inquiries, or investigations, enforcement actions, and other claims and liabilities, all of which may be costly and burdensome and further harm our reputation. Because techniques used to obtain unauthorized access or to sabotage systems change frequently and generally are not recognized until after they are launched against a target, we and our service providers may be unable to anticipate these techniques or to implement adequate preventative measures. Moreover, if a high- profile cybersecurity incident occurs with respect to another SaaS provider, customers may lose trust in the security of the SaaS business model generally, which could adversely affect our ability to retain existing customers or attract new ones. In the last few years there have been many successful advanced cybersecurity incidents that have damaged several prominent companies ~~in spite~~ **despite** ~~of~~ strong information security measures. We expect that the risks associated with cybersecurity incidents and the costs of preventing such attacks will continue to increase in the future. In addition, we cannot assure you that any limitation of liability provisions in our customer agreements, contracts with third- party vendors and service providers, or other contracts would be enforceable or adequate or would otherwise protect us from any liabilities or damages with respect to any particular claim relating to a security breach or other security- related matter or as a result of federal, state, or local laws or ordinances, or unfavorable judicial decisions in the **US,** ~~U. S.~~ or other countries. We maintain insurance to protect against certain

claims associated with the use of our platform, but our insurance coverage may not adequately cover any claim asserted against us. In addition, even claims that ultimately are unsuccessful could result in our expenditure of funds in litigation, divert management' s time and other resources, and harm our reputation. We also cannot be certain that our insurance coverage will be adequate for data handling or data security liabilities actually incurred, that insurance will continue to be available to us on economically reasonable terms, or at all, or that any future claim will not be excluded or otherwise be denied coverage by any insurer. The successful assertion of one or more large claims against us that exceed available insurance coverage, or the occurrence of changes in our insurance policies, including premium increases or the imposition of large deductible or co-insurance requirements, could adversely affect our business, operating results **, and financial condition. Existing and future acquisitions, strategic investments, partnerships or alliances could be difficult to identify and integrate, divert the attention of key management personnel, disrupt our business, dilute stockholder value and adversely affect our business, operating results,** and financial condition. As part of our business strategy, we have in the past and expect to continue to make investments in and / or acquire complementary companies, services, products, technologies, or talent. For example, in February 2021 we acquired Scalyr, a data analytics company ~~and~~ **,** in May 2022 we acquired Attivo, a leading identity security and lateral movement protection **company, in November 2023 we acquired KSG, a strategic advisory group, and in February 2024 we acquired both PingSafe, a cloud security platform, and Stride, a security automation** company. We have also invested in certain privately held companies through our S Ventures fund **, and we may not realize a return on these investments. All of our venture investments are subject to a risk of partial or total loss of investment capital** . Our ability as an organization to acquire and integrate other companies, services or technologies in a successful manner is not guaranteed. In the future, we may not be able to find suitable acquisition candidates, and we may not be able to complete such acquisitions on favorable terms, if at all. Our due diligence efforts may fail to identify all of the challenges, problems, liabilities or other shortcomings involved in an acquisition. If we do complete acquisitions, we may not ultimately strengthen our competitive position or ability to achieve our business objectives, and any acquisitions we announce or complete could be viewed negatively by our customers or investors. In addition, if we are unsuccessful at integrating existing and future acquisitions, or the technologies and personnel associated with such acquisitions, into our company, the revenue and operating results of the combined company could be adversely affected. Any integration process may require significant time and resources, and we may not be able to manage the process successfully. We may not successfully evaluate or utilize the acquired technology or personnel, or accurately forecast the financial impact of an acquisition transaction, causing unanticipated write- offs or accounting charges. Additionally, integrations could take longer than expected, or if we move too quickly in trying to integrate an acquisition, strategic investment, partnership, or other alliance, we may fail to achieve the desired efficiencies. We have, and may in the future have, to pay cash, incur debt **,** or issue equity securities to pay for any such acquisition, each of which could adversely affect our financial condition and the market price of our Class A common stock. The sale of equity or issuance of debt to finance any such acquisitions could result in dilution to our stockholders, which depending on the size of the acquisition, may be significant. The incurrence of indebtedness would result in increased fixed obligations and could also include covenants or other restrictions that would impede our ability to manage our operations. Additional risks we may face in connection with acquisitions include: • diversion of management' s time and focus from operating our business to addressing acquisition integration challenges; • the inability to coordinate research and development and sales and marketing functions; • the inability to integrate product and service offerings; • retention of key employees from the acquired company; • changes in relationships with strategic partners or the loss of any key customers or partners as a result of product acquisitions or strategic positioning resulting from the acquisition; • cultural challenges associated with integrating employees from the acquired company into our organization; • integration of the acquired company' s accounting, ~~CRM~~ **customer relationship management** , management information, human resources and other administrative systems; • the need to implement or improve controls, procedures and policies at a business that prior to the acquisition may have lacked sufficiently effective controls, procedures and policies; • unexpected security risks or higher than expected costs to improve the security posture of the acquired company; • higher than expected costs to bring the acquired company' s IT infrastructure up to our standards; • additional legal, regulatory **,** or compliance requirements; • financial reporting, revenue recognition or other financial or control deficiencies of the acquired company that we don' t adequately address and that cause our reported results to be incorrect; • liability for activities of the acquired company before the acquisition, including intellectual property infringement claims, violations of laws, commercial disputes, tax liabilities **,** and other known and unknown liabilities; • failing to achieve the expected benefits of the acquisition or investment; and • litigation or other claims in connection with the acquired company, including claims from or against terminated employees, customers, current and former stockholders **,** or other third parties. Our failure to address these risks or other problems encountered in connection with acquisitions and investments could cause us to fail to realize the anticipated benefits of these acquisitions or investments, cause us to incur unanticipated liabilities, and harm our business generally. **Historically** ~~In recent periods~~ , we have experienced rapid growth in the adoption of our platform, customer base **,** and revenue. However, we may not ~~continue~~ **return** to **our prior** ~~grow~~ **growth rates** or grow at the same rate in the future. Any success that we may experience in the future will depend, in large part, on our ability to, among other things: • maintain, renew and expand our existing customer base; • continue to attract new customers; • induce customers to expand deployment of the initially adopted module (s) of our platform across their organizations and infrastructure, and to adopt additional modules of our platform and services; • improve the capabilities of our platform through research and development; • continue to successfully expand our business domestically and internationally; and • successfully compete with other companies in the endpoint security industry. Our customers have no obligation to renew their subscription for our platform after the expiration of their contractual subscription period, which is generally one to three years, and in the normal course of business, some customers have elected not to renew. In addition, our customers may renew for shorter contract subscription lengths or cease using certain features. Our customer retention and expansion may decline or fluctuate as a result of a number of factors, including our customers' satisfaction with our services, our

pricing, customer security and networking issues and requirements, our customers' spending levels, decreases in the number of endpoints to which our customers deploy our solution, mergers and acquisitions involving our customers, industry developments, competition, general economic conditions, or the perceived decline in the incidence of cyberattacks. If our efforts to maintain and expand our relationships with our existing customers are not successful, our business, operating results, and financial condition will materially suffer. If our platform is not effectively interoperated within our customers' IT infrastructure, deployments could be delayed or canceled, which would adversely impact our business, operating results, and financial condition. Our platform must effectively interoperate with our customers' existing IT infrastructure, which often has different specifications, utilizes multiple protocol standards, deploys products and services from multiple vendors, and contains multiple generations of products and services that have been added over time. As a result, our solutions can sometimes encounter interoperability issues on deployment or over time, which require additional support and problem solving with customers, in some cases, at a substantial cost to us. We may modify our software or introduce new capabilities so that our platform interoperates with a customer' s infrastructure. These issues could cause longer deployment and integration times for our platform, leading to customer churn, which would adversely affect our business, operating results, and financial condition. In addition, government and other customers may require our platform to comply with certain security or other certifications and standards. If we are unable to achieve, or are delayed in achieving, compliance with these certifications and standards, we may be disqualified from selling our platform to such customers, or may otherwise be at a competitive disadvantage, either of which could adversely affect our business, operating results, and financial condition. Disruptions or other business interruptions that affect the availability of our platform could adversely impact our customer relationships and overall business. Our platform is hosted by third- party cloud hosting providers including ~~Amazon Web Services (~~AWS ~~)~~. Our software and systems are designed to use computing, storage capabilities, bandwidth, and other services provided by such cloud hosting providers, and currently our cloud service infrastructure is primarily run on AWS. We have experienced, and expect in the future that we may experience from time to time, interruptions, delays or outages in service availability due to a variety of factors. Capacity constraints could arise from a number of causes such as technical failures, natural disasters, fraud, or security attacks. The level of service provided by our cloud hosting providers, or regular or prolonged interruptions in that service, could also impact the use of, and our customers' satisfaction with, our platform and could harm our business and reputation. In addition, hosting costs are expected to increase as our customer base grows, which could adversely affect our business, operating results **,** and financial condition. Furthermore, AWS has discretion to change and interpret its terms of service and other policies with respect to us, including on contract renewal, and those actions may be unfavorable to our business operations. AWS, and other cloud hosting providers, may also take actions beyond our control that could seriously harm our business, including discontinuing or limiting our access to one or more services, increasing pricing terms, competing with us, terminating or seeking to terminate our contractual relationship altogether, or altering how we are able to process data on their system in a way that is unfavorable or costly to us. Although we obtain services from other cloud hosting providers, if our current arrangement with AWS were **to be** terminated, we could experience interruptions on our platform and in our ability to make our content available to customers, as well as delays and additional expenses in arranging for expansion and transition to alternative cloud hosting and infrastructure services. Such a transition could require further technical changes to our platform, including, but not limited to, our cloud service infrastructure which was initially designed to run on AWS. Making such changes could be costly in terms of time and financial resources. Any of these factors could reduce our revenue, subject us to liability, and cause our customers to decline to renew their subscriptions, any of which would harm our business and operating results. We may not timely and cost- effectively scale and adapt our existing technology to meet our customers' performance and other requirements. Our future growth is dependent upon our ability to continue to meet the needs of new customers and the expanding needs of our existing customers as their use of our solutions grows. As our customers gain more experience with our platform, the number of endpoints and events, the amount of data transferred, processed and stored by us, and the number of locations where our platform is being accessed, have in the past, and may in the future, expand rapidly. In order to meet the performance and other requirements of our customers, we intend to continue to make significant investments to increase capacity and to develop and implement new technologies in our service and cloud infrastructure operations. These technologies, which include databases, applications, and server optimizations, network and hosting strategies, and automation, are often advanced, complex, new and untested. We may not be successful in developing or implementing these technologies. In addition, it takes a significant amount of time to plan, develop and test improvements to our technologies and infrastructure, and we may not be able to accurately forecast demand or predict the results we will realize from such improvements. In some circumstances, we may also determine to scale our technology through the acquisition of complementary businesses and technologies rather than through internal development, which may divert management' s time and resources. To the extent that we do not effectively scale our operations to meet the needs of our growing customer base and to maintain performance as our customers expand their use of our solution, we will not be able to grow as quickly as we anticipate, our customers may reduce or cancel use of our solutions and we will be unable to compete as effectively and our business and operating results will be adversely affected. If we do not accurately anticipate and promptly respond to changes in our customers' technologies, business plans or security needs, our competitive position and prospects will be adversely impacted. The cybersecurity market has grown quickly and is expected to continue to evolve rapidly. Moreover, many of our customers operate in markets characterized by rapidly changing technologies and business plans, which require them to add numerous network- connected endpoints and adapt to increasingly complex IT environments, incorporating a variety of hardware, software applications, operating systems, and networking protocols. As their technologies and business plans grow more complex, we expect these customers to face new and increasingly sophisticated methods of attack. We face significant challenges in ensuring that our platform effectively identifies and responds to these advanced and evolving attacks **, including as a result of the evolving AI landscape** . As a result of the continued rapid innovations in the technology industry, including the rapid growth of smartphones, tablets and other devices, enterprise employees using personal devices for work, ~~and~~

the rapidly evolving Internet of Things **and AI** , we expect the networks of our customers to continue to change rapidly and become more complex. There can be no assurance that we will be successful in developing and marketing, on a timely basis, enhancements to our platform that adequately address the changing needs of our customers. In addition, any enhancements to our platform could involve research and development processes that are more complex, expensive and time- consuming than we anticipate. We may experience unanticipated delays in the availability of enhancements to our platform and may fail to meet customer expectations with respect to the timing of such availability. If we do not quickly respond to the rapidly changing and rigorous needs of our customers by developing and releasing updates to our platform on a timely basis that can adequately respond to advanced threats and our customers' evolving needs, our business, operating results, and financial condition will be adversely affected. If we are not able to maintain and enhance our brand and reputation, our business and operating results may be adversely affected. We believe that maintaining and enhancing our brand and our reputation as a leading provider of endpoint **and platform** security solutions is critical to our relationship with our existing customers, channel partners, and alliance partners and our ability to attract new customers and partners. The successful promotion of our brand will depend on a number of factors, including our ability to continue to develop additional features for our platform, our ability to successfully differentiate our platform from competitive cloud- based or legacy security solutions, our marketing efforts, and, ultimately, our ability to detect and stop breaches. Although we believe it is important for our growth, our brand promotion activities may not be successful or yield increased revenue. Under certain circumstances, our employees may have access to our customers' platforms. An employee may take advantage of such access to conduct malicious activities. Any such misuse of our platform could result in negative press coverage and negatively affect our reputation, which could result in harm to our business, reputation, and operating results. In addition, independent industry and research firms often evaluate our solutions and provide reviews of our platform, as well as the products of our competitors, and perception of our platform in the marketplace may be significantly influenced by these reviews. If these reviews are negative, or less positive as compared to those of our competitors' products, our brand may be adversely affected. Our solutions may fail to detect or prevent threats in any particular test for a number of reasons that may or may not be related to the efficacy of our solutions in real world environments. To the extent potential customers, industry analysts or research firms believe that the occurrence of a failure to detect or prevent any particular threat is a flaw or indicates that our solutions or services do not provide significant value, we may lose customers, and our reputation, financial condition and business would be harmed. Moreover, the performance of our channel partners and alliance partners may affect our brand and reputation if customers do not have a positive experience with these partners. In addition, we have in the past worked, and continue to work, with high profile customers as well as assist in analyzing and remediating high profile cyberattacks. Our work with such customers has exposed us to publicity and media coverage. Negative publicity about us, including about our management, the efficacy and reliability of our platform, our products offerings, our professional services, and the customers we work with, even if inaccurate, could adversely affect our reputation and brand. Substantially all of our sales are fulfilled through our channel partners, including resellers, distributors, MSPs, MSSPs, MDRs, OEMs, and IR firms, and we expect that we will continue to generate a significant portion of our revenue from channel partners for the foreseeable future. Our **agreements with our** channel partners ~~generated 90 %, 92 %, and 96 % of our revenue for fiscal 2023, 2022, and 2021, respectively. Our largest channel partner for fiscal 2023, 2022, and 2021, was Exclusive Networks. We generated 18 %, 18 %, and 19 % of our revenue from Exclusive Networks for fiscal 2023, 2022, and 2021, respectively. Our agreements with our channel partners, including agreements with Exclusive Networks,~~ are non- exclusive, do not last for set terms, and may be terminated by either party at any time. Further, channel partners fulfill our sales on a purchase order basis and do not impose minimum purchase requirements or related terms on sales. Additionally, we have entered, and intend to continue to enter, into alliance partnerships with third parties to support our future growth plans. The loss of a substantial number of our channel partners or alliance partners, or the failure to recruit additional partners, would adversely affect our business, operating results, and financial condition. To the extent our partners are unsuccessful in selling our platform, or if we are unable to enter into arrangements with and retain a sufficient number of high- quality partners in each of the regions in which we sell or plan to sell our platform, we are unable to keep them motivated to sell our platform, or our partners shift focus to other vendors and / or our competitors, our ability to sell our platform and operating results will be harmed. The termination of our relationship with any significant partner may adversely affect our sales and operating results. Our ability to achieve revenue growth in the future will depend in part on our ability to maintain successful relationships with our channel partners and in training our channel partners to independently sell and deploy our platform. We are also exposed to credit and liquidity risks and our operating results will be harmed if our partners were to become unable or unwilling to pay us at all or in a timely manner, terminate their relationships with us or go out of business. Although we have programs in place that are designed to monitor and mitigate such risks, we cannot guarantee these programs will be effective in reducing our risks. If we are unable to adequately control these risks, our business, operating results, and financial condition would be harmed. If partners fail to pay us under the terms of our agreements or we are otherwise unable to collect on our accounts receivable from these partners, we may be adversely affected both from the inability to collect amounts due and the cost of enforcing the terms of our contracts, including litigation. Our partners may seek bankruptcy protection or other similar relief and fail to pay amounts due to us, or pay those amounts more slowly, either of which would adversely affect our business, operating results, and financial condition. We may be further impacted by consolidation of our existing channel partners. In such instances, we may experience changes to our overall business and operational relationships due to dealing with a larger combined entity, and our ability to maintain such relationships on favorable contractual terms may be more limited. We may also become increasingly dependent on a more limited number of channel partners, as consolidation increases the relative proportion of our business for which each channel partner is responsible, which may magnify the risks described in the preceding paragraphs. Our business depends, in part, on sales to government organizations, and significant changes in the contracting or fiscal policies of such government organizations could adversely affect our business and operating results. Our future growth depends, in part, on increasing sales to government

organizations. Demand from government organizations is often unpredictable and subject to budgetary uncertainty. We have made significant investments to address the government sector, but we cannot assure you that these investments will be successful, or that we will be able to maintain or grow our revenue from the government sector. Although we anticipate that they may increase in the future, sales to governmental organizations have not accounted for, and may never account for, a significant portion of our revenue. Sales to governmental organizations are subject to a number of challenges and risks that may adversely affect our business and operating results, including the following risks: • selling to governmental agencies can be highly competitive, expensive, and time consuming, often requiring significant upfront time and expense without any assurance that such efforts will generate a sale; • government certification, software supply chain or source code transparency requirements applicable to us or our platform may change and, in doing so, restrict our ability to sell into the governmental sector until we have attained the revised certification or meet other new requirements. For example, although ~~SentinelOne is~~ **we are** currently FedRAMP authorized, such authorization is costly to maintain and subject to rigorous compliance and if we lose our authorization, it ~~would~~ **will** restrict our ability to sell to government customers; • government demand and payment for our platform may be impacted by public sector budgetary cycles and funding authorizations, with funding reductions or delays adversely affecting public sector demand for our platform, including as a result of sudden, unforeseen and disruptive events such as government ~~shut downs~~ **shutdowns, governmental defaults on indebtedness** , war **, regional geopolitical conflicts around the world** , incidents of terrorism, natural disasters, and public health concerns or epidemics; • governments routinely investigate and audit government contractors' administrative processes, and any unfavorable audit could result in the government refusing to continue buying our platform, which would adversely impact our revenue and operating results, or institute fines or civil or criminal liability if an investigation, audit, or other review, were to uncover improper or illegal activities; • governments may require certain products to be manufactured, produced, hosted or accessed solely in their country or in other relatively high- cost locations, and we may not produce or host all products in locations that meet these requirements, affecting our ability to sell these products to governmental agencies; and • refusal to grant certain certifications or clearance by one government agency, or decision by one government agency that our products do not meet certain standards, may cause reputational harm and cause concern with other government agencies. The occurrence of any of the foregoing could cause governmental organizations to delay or refrain from purchasing our solutions in the future or otherwise adversely affect our business and operating results. Our long- term success depends, in part, on our ability to expand the sale of our platform to customers located outside of the **US** ~~United States~~ and our current, and any further, expansion of our international operations exposes us to risks that could have a material adverse effect on our business, operating results, and financial condition. We are generating a growing portion of our revenue outside of the **US** ~~United States~~ , and conduct our business activities in various foreign countries, including some emerging markets where we have limited experience, where the challenges of conducting our business can be significantly different from those we have faced in more developed markets and where business practices may create internal control risks including: • fluctuations in foreign currency exchange rates, which could add volatility to our operating results; • new, or changes in, regulatory requirements; • tariffs, export and import restrictions, restrictions on foreign investments, sanctions, and other trade barriers or protection measures; • exposure to numerous, increasing, stringent (particularly in the **EU** ~~European Union~~), and potentially inconsistent laws and regulations relating to privacy, data protection, and information security; • costs of localizing products and services **(including, but not limited to data localization requirements)** ; • lack of acceptance of localized products and services; • the need to make significant investments in people, solutions and infrastructure, typically well in advance of revenue generation; • challenges inherent in efficiently managing an increased number of employees over large geographic distances, including the need to implement appropriate systems, policies, benefits, and compliance programs; • difficulties in maintaining our corporate culture with a dispersed and distant workforce; • treatment of revenue from international sources, evolving domestic and international tax environments, and other potential tax issues, including with respect to our corporate operating structure and intercompany arrangements; • different or weaker protection of our intellectual property, including increased risk of theft of our proprietary technology and other intellectual property; • economic weakness or currency- related crises; • compliance with multiple, conflicting, ambiguous or evolving governmental laws and regulations, including employment, tax, data privacy, anti- corruption, import / export, antitrust, data transfer, storage and protection, and industry- specific laws and regulations, including rules related to compliance by our third-party resellers and our ability to identify and respond timely to compliance issues when they occur **and regulations applicable to us and our third party data providers from whom we purchase and resell syndicated data** ; • vetting and monitoring our third- party channel partners in new and evolving markets to confirm they maintain standards consistent with our brand and reputation; • generally longer payment cycles and greater difficulty in collecting accounts receivable; • our ability to adapt to sales practices and customer requirements in different cultures; • the lack of reference customers and other marketing assets in regional markets that are new or developing for us, as well as other adaptations in our market generation efforts that we may be slow to identify and implement; • dependence on certain third parties, including channel partners with whom we do not have extensive experience; • natural disasters, acts of war, terrorism, or pandemics, including the **armed** ~~COVID- 19 pandemic and the conflict~~ **conflicts** in **the Middle East,** Ukraine **and tensions between China and Taiwan** ; • **actual or perceived** instability in the global banking system **; • cybersecurity incidents** ; • corporate espionage; and • political instability and security risks in the countries where we are doing business and changes in the public perception of governments in the countries where we operate or plan to operate. We have undertaken, and will continue to undertake, additional corporate operating restructurings from time to time that involve our group of foreign country subsidiaries through which we do business abroad. We consider various factors in evaluating these restructurings, including the alignment of our corporate legal entity structure with our organizational structure and its objectives, the operational and tax efficiency of our group structure, and the long- term cash flows and cash needs of our business. Such restructurings increase our operating costs, and if ineffectual, could increase our income tax liabilities and our global effective tax rate. We have experienced rapid growth in recent periods, and if we do not

effectively manage our future growth, our business, operating results, and financial condition may be adversely affected. We have experienced rapid growth in recent periods, and we expect to continue to invest broadly across our organization to support our growth. For example, our headcount grew from over ~~1, 200 employees as of January 31, 2022, to over~~ 2, 100 employees as of January 31, 2023 **, to over 2, 300 employees as of January 31, 2024** . Although we have experienced rapid growth historically, we may not sustain our ~~current~~ growth rates, nor can we assure you that our investments to support our growth will be successful. The growth and expansion of our business will require us to invest significant financial and operational resources and the continuous dedication of our management team. In addition, as we have grown, our number of customers has also increased significantly, and we have increasingly managed more complex deployments of our platform in more complex computing environments. The rapid growth and expansion of our business places a significant strain on our management, operational, and financial resources. To manage any future growth effectively, we must continue to improve and expand our information technology and financial infrastructure, our operating and administrative systems and controls, and our ability to manage headcount, capital, and processes in an efficient manner **. As a result of recent macroeconomic conditions, in June 2023, we approved a restructuring plan designed to improve operational efficiencies and operating costs and better align our workforce and operations with current business needs, priorities, and near- term growth expectations** . If we continue to experience rapid growth, we may not be able to successfully implement or scale improvements to our systems, processes, and controls in an efficient or timely manner. For example, as we grow, we may experience difficulties in managing improvements to our systems, processes, and controls or in connection with third- party software licensed to help us with such improvements. As we grow, our existing systems, processes, and controls may not prevent or detect all errors, omissions, or fraud. Any future growth will continue to add complexity to our organization and require effective coordination throughout our organization. Failure to manage any future growth effectively could result in increased costs, cause difficulty or delays in deploying new customers, reduce demand for our platform, cause difficulties in introducing new features or other operational difficulties, and any of these difficulties would adversely affect our business, operating results, and financial condition. Our sales cycles can be long and unpredictable, and our sales efforts require considerable time and expense. Our revenue recognition is difficult to predict because of the length and unpredictability of the sales cycle for our platform, particularly with respect to large organizations and government entities. For example, in light of current macroeconomic conditions, we have observed a lengthening of the sales cycle for some prospective customers that we attribute to higher cost- consciousness around IT budgets **, which has become more pronounced recently** . Customers often view the subscription to our platform as a significant strategic decision and, as a result, frequently require considerable time to evaluate, test and qualify our platform prior to entering into or expanding a relationship with us. Large enterprises and government entities in particular ~~,~~ often undertake a significant evaluation process that further lengthens our sales cycle. Our direct sales team develops relationships with our customers, and works with our channel partners on account penetration, account coordination, sales and overall market development. We spend substantial time and resources on our sales efforts without any assurance that our efforts will produce a sale. Security solution purchases are frequently subject to budget constraints, multiple approvals and unanticipated administrative, processing and other delays. As a result, it is difficult to predict whether and when a sale will be completed. The failure of our efforts to secure sales after investing resources in a lengthy sales process would adversely affect our business, operating results **,** and financial condition. The sales prices of our platform may decrease, or the mix of our sales may change, which may reduce our gross profits and adversely affect our business, operating results, and financial condition. We have limited experience with respect to determining the optimal prices for our platform. As the market for endpoint security matures, or as new competitors introduce new products or services that are similar to or compete with ours, we may be unable to effectively optimize our prices through increases or decreases, attract new customers at our offered prices or based on the same pricing model as we have used historically. Further, competition continues to increase in the market segments in which we participate, and we expect competition to further increase in the future, thereby leading to increased pricing pressures. Larger competitors with more diverse product and service offerings may reduce the price of products or services that compete with ours or may bundle them with other products and services. This could lead customers to demand greater price concessions or additional functionality at the same price levels. As a result, in the future we may be required to reduce our prices or provide more features without corresponding increases in price, which would adversely affect our business, operating results, and financial condition. Because we recognize revenue from subscriptions to our platform over the term of the subscription, downturns or upturns in new business will not be immediately reflected in our operating results. We generally recognize revenue from customers ratably over the term of their subscription, which is generally one to three years. As a result, a substantial portion of the revenue we report in each period is attributable to the recognition of deferred revenue relating to agreements that we entered into during previous periods. Consequently, any increase or decrease in new sales or renewals in any one period will not be immediately reflected in our revenue for that period. Any such change, however, would affect our revenue in future periods. Accordingly, the effect of downturns or upturns in new sales and potential changes in our rate of renewals will not be fully reflected in our operating results until future periods. We may also be unable to timely reduce our cost structure in line with a significant deterioration in sales or renewals that would adversely affect our business, operating results, and financial condition. We provide service level commitments under some of our customer contracts. If we fail to meet these contractual commitments, we could be obligated to provide partial refunds or our customers could be entitled to terminate their contracts and our business would suffer. Certain of our customer agreements contain service level commitments, which contain specifications regarding the availability of our platform and our support services. Failure of or disruption to our infrastructure or third- party hosting service providers could impact the performance of our platform and the availability of services to customers. If we are unable to meet our stated service level commitments or if we suffer extended periods of poor performance or unavailability of our platform, we may be contractually obligated to provide affected customers with credit, partial refunds or termination rights. To date, there has not been a material failure to meet our service level commitments, and we do not currently have any material liabilities accrued on

our consolidated balance sheets for such commitments. Our business, operating results, and financial condition would be adversely affected if we suffer performance issues or downtime that exceeds the service level commitments under our agreements with our customers. Our business is subject to the risks of warranty claims, product returns and product defects from real or perceived defects in our solutions or their misuse by our customers or third parties and indemnity provisions in various agreements potentially expose us to substantial liability for intellectual property infringement and other losses. We may be subject to liability claims for damages related to errors or defects in our solutions. A material liability claim or other occurrence that harms our reputation or decreases market acceptance of our platform will harm our business and operating results. Although we generally have limitation of liability provisions in our terms and conditions of sale, they may not fully or effectively protect us from claims as a result of federal, state or local laws or ordinances, or unfavorable judicial decisions in the **US** ~~United States~~ or other countries. The sale and support of our platform also entails the risk of product liability claims. We employ measures in the form of policy and technical controls to limit unauthorized access to our platform by our employees, customers and third **-** parties, however, these measures may not fully or effectively protect our platform from unauthorized access. Additionally, we typically provide indemnification to customers, partners or other third parties we do business with for certain losses suffered or expenses incurred as a result of third- party claims arising from our infringement of a third party' s intellectual property. We also provide unlimited liability for certain breaches of confidentiality, as defined in our master subscription agreement. We also provide limited liability in the event of certain breaches of our master subscription agreement. Certain of these contractual provisions survive termination or expiration of the applicable agreement. ~~To date, we have not incurred any material costs because of such obligations.~~ However, as we continue to grow, indemnification claims against us for the obligations listed ~~will~~ **may** increase. When our customers or other third parties we do business with make intellectual property rights or other indemnification claims against us, we ~~will~~ incur significant legal expenses and may have to pay damages, license fees and / or stop using technology found to be in violation of the third party' s rights. We may also have to seek a license for the technology. Such licenses may not be available on reasonable terms, if at all, and may significantly increase our operating expenses or may require us to restrict our business activities and limit our ability to deliver certain solutions or features. We may also be required to develop alternative non- infringing technology, which could require significant effort and expense and / or cause us to alter our platform, which could harm our business. Large indemnity obligations, whether for intellectual property or in certain limited circumstances, other claims, would harm our business, operating results and financial condition. Additionally, our platform may be used by our customers and other third parties who obtain access to our solutions for purposes other than for which our platform was intended. We maintain insurance to protect against certain claims associated with the use of our platform, but our insurance coverage may not adequately cover the claims asserted against us. In addition, even claims that ultimately are unsuccessful could result in our expenditure of funds in litigation, divert management' s time and other resources, and harm our business and reputation. We have offered some of our customers a limited warranty, subject to certain conditions. Any failure or refusal of our insurance providers to provide the expected insurance benefits to us after we have remediated warranty claims would cause us to incur significant expense or cause us to cease offering warranties which could damage our reputation, cause us to lose customers, expose us to liability claims by our customers, negatively impact our sales and marketing efforts, and have an adverse effect on our business, operating results, and financial condition. Further, although the terms of the warranty do not allow those customers to use warranty claim payments to fund payments to persons on the **US** ~~U. S.~~ Treasury Department' s Office of Foreign Assets Control (OFAC), list of Specially Designated Nationals and Blocked Persons or who are otherwise subject to **US** ~~U. S.~~ sanctions, we cannot assure you that all of our customers will comply with our warranty terms or refrain from taking actions, in violation of our warranty and applicable law **. Key business metrics and other estimates are subject to inherent challenges in measurement and to change as our business evolves, and our business, operating results, and financial condition could be adversely affected by real or perceived inaccuracies in those metrics or any changes in metrics we disclose. We regularly review key business metrics, including our ARR, number of customers with ARR of $ 100, 000, NRR, and other measures to evaluate growth trends, measure our performance, and make strategic decisions. These key metrics are calculated using internal company data and have not been validated by an independent third party. While these numbers are based on what we believe to be reasonable estimates for the applicable period of measurement at the time of reporting, there are inherent challenges in such measurements. If we fail to maintain effective processes and systems, our key metrics calculations may be inaccurate, and we may not be able to identify those inaccuracies. We regularly review our processes for calculating these metrics, and from time to time we make adjustments to improve their accuracy. Moreover, we may periodically change the definition or methodology underlying our key metrics. For example, as a result of a decline in usage and consumption in the quarter ended April 30, 2023, we decided to change our methodology of calculating ARR for consumption and usage- based agreements to reflect committed contract values as opposed to based on consumption and usage. In addition, as part of our quarterly review of ARR in connection with the preparation of our condensed consolidated financial statements for the quarter ended April 30, 2023, we discovered some historical inaccuracies relating to ARR on certain contracts, which we have corrected. As a result, we made a one- time adjustment of approximately 5 % of total ARR, which we reflected in our total ARR as of April 30, 2023. If our key metrics are inaccurate or if investors perceive any changes to our key business metrics or the methodologies for calculating these metrics negatively, our business could be adversely affected** . Risks Related to our People Our future success is dependent, in part, on our ability to hire, integrate, train, manage, retain, and motivate the members of our management team and other key employees throughout our organization. The loss of key personnel, including key members of our management team or members of our board of directors, as well as certain of our key marketing, sales, finance, support, product development, people team, or technology personnel, could disrupt our operations and have an adverse effect on our ability to grow our business. In particular, we are highly dependent on the services of Tomer Weingarten, our co- founder, Chairman of the Board of Directors, President, and Chief Executive Officer, who is critical to the development of our

technology, platform, future vision, and strategic direction. From time to time, there have been and may in the future be changes in our management team. While we seek to manage any such transitions carefully, such changes may result in a loss of institutional knowledge, cause disruptions to our business and negatively affect our business **. Further, we maintain an office in Tel Aviv, Israel and had approximately 13 % of our personnel in Israel as of January 31, 2024. We are closely monitoring the unfolding events of the armed conflict in Israel which began in October 2023. While this conflict is still evolving, to date, the conflict has not had an adverse impact on our workforce and we have implemented continuity measures to address the safety of our employees and continue our operations in the event of reduced employee availability in the conflict region. However, if our continuity measures fail or the conflict continues to worsen or intensify, any business interruptions or spillover effects could adversely affect our business and operations** . Competition for highly skilled personnel is intense, especially in the San Francisco Bay Area ~~and in Israel~~ , where we have a substantial presence and need for highly skilled personnel, and we may not be successful in hiring or retaining qualified personnel to fulfill our current or future needs. More generally, the technology industry, and the cybersecurity industry more specifically, is also subject to substantial and continuous competition for engineers with high levels of experience in designing, developing and managing software and related services. Moreover, the industry in which we operate generally experiences high employee attrition. We have, from time to time, experienced, and we expect to continue to experience, difficulty in hiring and retaining highly skilled employees with appropriate qualifications. For example, in recent years, recruiting, hiring and retaining employees with expertise in the cybersecurity industry has become increasingly difficult as the demand for cybersecurity professionals has increased as a result of ~~the~~ recent cybersecurity attacks on global corporations and governments. We may be required to provide more training to our personnel than we currently anticipate. Further, labor is subject to external factors that are beyond our control, including our industry' s highly competitive market for skilled workers and leaders, cost inflation, ~~the continuing effects of the COVID- 19 pandemic,~~ overall macroeconomics and workforce participation rates. **Should our competitors recruit our employees, our level of expertise and ability to execute our business plan would be negatively impacted. In June 2023, we approved a restructuring plan, which impacted approximately 5 % of our workforce. This reduction may adversely impact our ability to achieve our future operational targets. In the future, we may be unable to hire qualified employees and may be unable to successfully train those employees that we are able to hire, and as a result, employees may not become fully productive on the timelines that we have projected or at all. Further, the reduction could yield unanticipated consequences or disruptions in our day- to- day operations, such as attrition beyond planned staff reductions. Additionally,** ~~Restrictive~~ **restrictive** immigration policies or legal or regulatory developments relating to immigration may also negatively affect our efforts to attract and hire new personnel as well as retain our existing personnel. Changes in **US** ~~U. S.~~ immigration and work authorization laws and regulations can be significantly affected by political forces and levels of economic activity. Our business may be adversely affected if legislative or administrative changes to immigration or visa laws and regulations impair our hiring processes. Moreover, many of the companies with which we compete for experienced personnel have greater resources than we have. Our competitors also may be successful in recruiting and hiring members of our management team, sales team or other key employees, and it may be difficult for us to find suitable replacements on a timely basis, on competitive terms, or at all. We have in the past, and may in the future, be subject to allegations that employees we hire have been improperly solicited, or that they have divulged proprietary or other confidential information or that their former employers own such employees' inventions or other work product, or that they have been hired in violation of non- compete provisions or non- solicitation provisions. In addition, job candidates and existing employees often consider the value of the equity awards and other compensation they receive in connection with their employment. If the perceived value of our compensatory package declines, it may adversely affect our ability to attract and retain highly skilled employees. If we fail to attract new personnel or fail to retain and motivate our current personnel, our business and future growth prospects would be severely harmed. Further, our competitors may be successful in recruiting and hiring members of our management team or other key employees, and it may be difficult for us to find suitable replacements on a timely basis, on competitive terms, or at all. In recent years, the increased availability of hybrid or remote working arrangements has expanded the pool of companies that can compete for our employees and employment candidates. Although we have entered into employment agreements with our key employees, these agreements are on an " at- will " basis, meaning they are able to terminate their employment with us at any time. If we fail to attract new personnel or fail to retain and motivate our current personnel, our business and future growth prospects would be severely harmed. If we do not effectively ~~hire,~~ integrate, train, manage, and retain ~~additional~~ sales personnel, and expand our sales and marketing capabilities, we may be unable to increase our customer base and increase sales to our existing customers. Our ability to increase our customer base and achieve broader market adoption of our platform will depend to a significant extent on our ability to continue to expand our sales and marketing operations. We have and plan to continue to dedicate significant resources to sales and marketing programs and to expand our sales and marketing capabilities to target additional potential customers, but there is no guarantee that we will be successful in attracting and maintaining additional customers. If we are unable to find efficient ways to deploy our sales and marketing investments or if our sales and marketing programs are not effective, our business and operating results would be adversely affected. Furthermore, we plan to continue expanding our sales force and there is significant competition for sales personnel with the skills and technical knowledge that we require. Our ability to achieve revenue growth will depend, in part, on our success in hiring, integrating, training, managing, and retaining sufficient numbers of sales personnel to support our growth, particularly in international markets. New hires require significant training and may take extended time before they are productive. Our recent hires and planned hires may not become productive as quickly as we expect, or at all, and we may be unable to hire or retain sufficient numbers of qualified individuals in the markets where we do business or plan to do business. Moreover, our international expansion may be slow or unsuccessful if we are unable to retain qualified personnel with international experience, language skills and cultural competencies in the geographic markets ~~in~~ which we target. If we are

unable to hire, integrate, train, manage, and retain a sufficient number of effective sales personnel, or the sales personnel we hire are not successful in obtaining new customers or increasing sales to our existing customer base, our business, operating results and financial condition will be adversely affected. Any inability to maintain a high- quality customer support organization could lead to a lack of customer satisfaction, which could hurt our customer relationships and adversely affect our business, operating results, and financial condition. Once our platform is deployed within our customers' computing environments, our customers rely on our technical support services to assist with service customization and optimization and to resolve certain issues relating to the implementation and maintenance of our platform and advanced services. If we do not effectively assist our customers in deploying our platform, succeed in helping our customers quickly resolve technical issues, or provide effective ongoing support, our ability to sell additional products and services as part of our platform to existing customers would be adversely affected and our reputation with potential customers could be damaged. In addition, our sales process is highly dependent on our product and business reputation and on positive recommendations, referrals, and peer promotions from our existing customers. Any failure to maintain high- quality technical support, or a market perception that we do not maintain high- quality support, could adversely affect our reputation, our ability to sell our services to existing and prospective customers, and our business, operating results and financial condition. We believe that our corporate culture has contributed to our success, and if we cannot maintain this culture as we grow, we could lose the innovation, creativity, and teamwork fostered by our culture, and our business may be harmed. We believe that our corporate culture has been, and will continue to be a key contributor to our success. If we do not continue to develop our corporate culture as we grow and evolve, it could harm our ability to foster the innovation, inclusion, creativity, and teamwork that we believe is important to support our growth. As we implement more complex organizational structures, we may find it increasingly difficult to maintain the beneficial aspects of our corporate culture, which could negatively impact our future success. We are also taking steps to develop a more inclusive and diverse workforce, however, there is no guarantee that we will be able to do so. ~~Risks Related to Our Intellectual Property~~ We rely primarily on patent, trademark, copyright and trade secrets laws, and confidentiality agreements and contractual provisions to protect our technology. Valid patents may not issue from our pending applications, and the claims eventually allowed on any patents may not be sufficiently broad to protect our technology or platform. Any issued patents may be challenged, invalidated or circumvented, and any rights granted under these patents may not actually provide adequate defensive protection or competitive advantages to us. Patent applications in the **US** ~~United States~~ are typically not published until at least 18 months after filing, or, in some cases, not at all, and publications of discoveries in industry- related literature lag behind actual discoveries. We cannot be certain that we were the first to make the inventions claimed in our pending patent applications or that we were the first to file for patent protection. Additionally, the process of obtaining patent protection is expensive and time- consuming, and we may not be able to prosecute all necessary or desirable patent applications at a reasonable cost or in a timely manner. In addition, recent changes to the patent laws in the **US** ~~United States~~ may bring into question the validity of certain software patents and may make it more difficult and costly to prosecute patent applications. Such changes may lead to uncertainties or increased costs and risks surrounding the prosecution, validity, ownership, enforcement, and defense of our issued patents and patent applications and other intellectual property, the outcome of third- party claims of infringement, misappropriation, or other violation of intellectual property brought against us and the actual or enhanced damages (including treble damages) that may be awarded in connection with any such current or future claims, and could have a material adverse effect on our business, operating results, and financial condition. Despite our efforts to protect our proprietary rights, unauthorized parties may attempt to copy aspects of our platform or obtain and use information that we regard as proprietary. We generally enter into confidentiality or license agreements with our employees, consultants, vendors, and customers, and generally limit access to and distribution of our proprietary information. However, such agreements may not be enforceable in full or in part in all jurisdictions and any breach could negatively affect our business and our remedy for such breach may be limited. The contractual provisions that we enter into may not prevent unauthorized use or disclosure of our proprietary technology or intellectual property rights and may not provide an adequate remedy in the event of unauthorized use or disclosure of our proprietary technology or intellectual property rights. Lastly, the measures we employ to limit the access and distribution of our proprietary information may not prevent unauthorized use or disclosure of our proprietary technology or intellectual property. As such, we cannot guarantee that the steps taken by us will prevent misappropriation of our technology. Policing unauthorized use of our technology or platform is difficult. In addition, the laws of some foreign countries do not protect our proprietary rights to the same extent as the laws of the **US** ~~United States~~, and many foreign countries do not enforce these laws as diligently as government agencies and private parties in the **US** ~~United States~~. For example, many foreign countries limit the enforceability of patents against certain third parties, including government agencies or government contractors. In these countries, patents may provide limited or no benefit. Effective trade secret protection may also not be available in every country in which our products are available or where we have employees or independent contractors. The loss of trade secret protection could make it easier for third parties to compete with our products by copying functionality. In addition, any changes in, or unexpected interpretations of, the trade secret and employment laws in any country in which we operate may compromise our ability to enforce our trade secret and intellectual property rights. From time to time, legal action by us may be necessary to enforce our patents and other ~~IP~~ **intellectual property** rights, to protect our trade secrets, to determine the validity and scope of the proprietary rights of others or to defend against claims of infringement or invalidity **. Moreover, the availability of copyright protection and other legal protections for intellectual property generated by certain technologies, such as generative AI, is uncertain. The use of generative AI and other forms of AI may expose us to risks because the intellectual property ownership and license rights, including copyright, of generative and other AI output, has not been fully interpreted by US courts or been fully addressed by US federal or state regulation, as well as in foreign jurisdictions** . Such litigation could result in substantial costs and diversion of resources and could negatively affect our business, operating results and financial condition. If we are unable to protect our proprietary rights (including aspects of our software and platform protected other than by patent rights), we will find ourselves

at a competitive disadvantage to others who need not incur the additional expense, time and effort required to create our platform and other innovative products that have enabled us to be successful to date. Moreover, we may need to expend additional resources to defend our intellectual property rights in foreign countries, and our inability to do so could impair our business or adversely affect our international expansion. Third parties have claimed and may claim that our platform infringes their intellectual property rights and this may create liability for us or otherwise adversely affect our business, operating results, and financial condition. Third parties have claimed, and may claim in the future, that our current or future products and services infringe their intellectual property rights, and such claims may result in legal claims against our channel partners, our alliance partners, our customers and us. These claims may damage our brand and reputation, harm our customer relationships, and create liability for us **. Contractually, we are expected to indemnify our partners and customers for these types of claims** . We expect the number of such claims to increase as the number of products and services and the level of competition in our market grows, as the functionality of our platform overlaps with that of other products and services, and as the volume of issued software patents and patent applications continues to increase. We generally agree in our customer and partner contracts to indemnify customers for certain expenses or liabilities they incur as a result of third- party intellectual property infringement claims associated with our platform. To the extent that any claim arises as a result of third- party technology we have licensed for use in our platform, we may be unable to recover from the appropriate third party any expenses or other liabilities that we incur. Companies in the software and technology industries, including some of our current and potential competitors, own large numbers of patents, copyrights, trademarks, and trade secrets and frequently enter into litigation based on allegations of infringement or other violations of intellectual property rights. In addition, many of these companies have the capability to dedicate substantially greater resources to enforce their intellectual property rights and to defend claims that may be brought against them. Furthermore, patent holding companies, non- practicing entities, and other adverse patent owners that are not deterred by our existing intellectual property protections may seek to assert patent claims against us. From time to time, third parties, including certain of these leading companies, have invited us to license their patents and may, in the future, assert patent, copyright, trademark, or other intellectual property rights against us, our channel partners, our alliance partners, or our customers. We have received, and may in the future receive, notices that claim we have misappropriated, misused, or infringed other parties' intellectual property rights, and, to the extent we gain greater market visibility, we face a higher risk of being the subject of intellectual property infringement claims ~~. In May 2021, and thereafter, we have received communications from International Business Machines Corporation (IBM), alleging that we infringe on U. S. patents held by IBM. We have also asserted that IBM infringes certain patents held by us. To date, no litigation has been filed in this matter. Based on our review of the patents at issue, we believe we have meritorious defenses to IBM' s allegations, although there can be no assurance that litigation will not commence, or that we will be successful in such litigation or reaching a business resolution that is satisfactory to us. In November 2022 we received communications from AT & T alleging that our platform integrated into an AT & T offering is subject to a third- party patent infringement claim and that we may be required to indemnify AT & T. To date, no litigation has been filed in this matter. Based on our review and analysis of the matter and allegations at issue, we are vigorously contesting the indemnity claim, although, there can be no assurances that litigation will not commence, that we will be successful in such litigation, or that we will reach a satisfactory business resolution~~ . There may be third- party intellectual property rights, including issued or pending patents and trademarks, that cover significant aspects of our technologies or business methods and assets. We may also face exposure to third- party intellectual property infringement, misappropriation, or violation actions if we engage software engineers or other personnel who were previously engaged by competitors or other third parties and those personnel inadvertently or deliberately incorporate proprietary technology of third parties into our products. In addition, we may lose valuable intellectual property rights or personnel. A loss of key personnel or their work product could hamper or prevent our ability to develop, market, and support potential products or enhancements, which could severely harm our business. Any intellectual property claims, with or without merit, could be very time- consuming, could be expensive to settle or litigate, and could divert our management' s attention and other resources. These claims could also subject us to significant liability for damages, potentially including treble damages if we are found to have willfully infringed patents or copyrights, and may require us to indemnify our customers for liabilities they incur as a result of such claims. These claims could also result in our having to stop using technology found to be in violation of a third party' s rights. We might be required to seek a license for the intellectual property, which may not be available on reasonable terms or at all. Even if a license were available, we could be required to pay significant royalties, which would increase our operating expenses. Alternatively, we could be required to develop alternative non- infringing technology, which could require significant time, effort, and expense, and may affect the performance or features of our platform. If we cannot license or develop alternative non- infringing substitutes for any infringing technology used in any aspect of our business, we would be forced to limit or stop sales of our platform and may be unable to compete effectively. Any of these results would adversely affect our business, operating results, and financial condition. We license technology from third parties, and our inability to maintain those licenses could harm our business. We currently incorporate, and will in the future incorporate, technology that we license from third parties, including software, into our solutions. Licensing technologies from third parties exposes us to increased risk of being the subject of intellectual property infringement and vulnerabilities due to, among other things, our lower level of visibility into the development process with respect to such technology and the care taken to safeguard against risks. We cannot be certain that our licensors do not or will not infringe on the intellectual property rights of third parties or that our licensors have or will have sufficient rights to the licensed intellectual property in all jurisdictions in which we may sell our platform. Some of our agreements with our licensors may be terminated by them for convenience, or otherwise provide for a limited term. If we are unable to continue to license technology because of intellectual property infringement claims brought by third parties against our licensors or against us, or if we are unable to continue our license agreements or enter into new licenses on commercially reasonable terms, our ability to develop and sell solutions and services containing or dependent on that technology would be

limited, and our business, including our financial conditions, cash flows and results of operations could be harmed. Additionally, if we are unable to license technology from third parties, we may be forced to acquire or develop alternative technology, which we may be unable to do in a commercially feasible manner, or at all, and may require us to use alternative technology of lower quality or performance standards. This could limit or delay our ability to offer new or competitive solutions and increase our costs. Third- party software we rely on may be updated infrequently, unsupported or subject to vulnerabilities that may not be ~~patched~~ **resolved** in a timely manner, any of which may expose our solutions to vulnerabilities. As a result, our business, operating results, and financial condition would be adversely affected. Some of our technology incorporates " open source " software, which could negatively affect our ability to sell our platform and subject us to possible litigation. Our platform contains third- party open source software components, and failure to comply with the terms of the underlying open source software licenses could restrict our ability to sell our products and subscriptions. The use and distribution of open source software may entail greater risks than the use of third- party commercial software, as open source licensors generally do not provide warranties or other contractual protections regarding infringement claims or the quality of the code, which they are not typically required to maintain and update, and they can change the license terms on which they offer the open source software. Although we monitor our use of open source software in an effort both to comply with the terms of the applicable open source licenses and to avoid subjecting our products to conditions we do not intend, many of the risks associated with use of open source software cannot be eliminated and could negatively affect our business. In addition, the wide availability of source code used in our solutions could expose us to security vulnerabilities. Some open source licenses contain requirements that we make available **as** source code for modifications or derivative works we create based upon our use and distribution of the open source software. If we combine and distribute our proprietary software with open source software in a certain manner, we could, under certain open source licenses, be required to release combined the source code of our proprietary software to the public, including authorizing further modification and redistribution, or otherwise be limited in the licensing of our services, each of which could provide an advantage to our competitors or other entrants to the market, create security vulnerabilities in our solution, require us to re- engineer all or a portion of our platform, and reduce or eliminate the value of our services. This would allow our competitors to create similar products with lower development effort and time and ultimately could result in a loss of sales for us. The terms of many open source licenses have not been interpreted by **US** ~~U. S.~~ courts, and there is a risk that these licenses could be construed in ways that could impose unanticipated conditions or restrictions on our ability to commercialize products and subscriptions incorporating such software. Moreover, we cannot assure you that our processes for controlling our use of open source software in our products and subscriptions will be effective. From time to time, we may face claims from third parties asserting ownership of, or demanding release of, the open source software or derivative works that we developed using such software (which could include our proprietary source code), or otherwise seeking to enforce the terms of the applicable open source license. These claims, regardless of validity, could result in time consuming and costly litigation, divert management' s time and attention away from developing the business, expose us to customer indemnity claims, or force us to disclose source code. Litigation could be costly for us to defend, result in paying damages, entering into unfavorable licenses, have a negative effect on our operating results and financial condition, or cause delays by requiring us to devote additional research and development resources to change our solution. Risks Related to Legal and Regulatory Matters We are subject to laws and regulations, including governmental export and import controls, sanctions and anti- corruption laws, that could impair our ability to compete in our markets and subject us to liability if we are not in full compliance with applicable laws. We are subject to laws and regulations, including governmental export and import controls, that could subject us to liability or impair our ability to compete in our markets. Our platform and related technology ~~is~~ **are** subject to **US** ~~U. S.~~ export controls, including the **US** ~~U. S.~~ Department of Commerce' s Export Administration Regulations (**also known as "** EAR **"**), and we and our employees, representatives, contractors, agents, intermediaries, and other third parties are also subject to various economic and trade sanctions regulations administered by OFAC and other **US** ~~U. S.~~ government agencies. We incorporate standard encryption algorithms into our platform, which, along with the underlying technology, may be exported outside of the **US** ~~U. S.~~ only with the required export authorizations, including by license, license exception or other appropriate government authorizations, which may require the filing of an encryption registration and classification request. We also offer certain customers a ransomware warranty in addition to their subscriptions, providing coverage in the form of a limited monetary payment if they are affected by a ransomware attack (as specified in our ransomware warranty agreement), and though the terms of the warranty do not allow those customers to use warranty claim payments to fund payments to persons on OFAC' s list of Specially Designated Nationals and Blocked Persons or who are otherwise prohibited to receive such payments under **US** ~~U. S.~~ sanctions, we cannot assure you that all of our customers will comply with our warranty terms or refrain from taking actions in violation of our warranty and applicable law. Furthermore, **US** ~~U. S.~~ export control laws and economic sanctions prohibit the export and re- export of certain hardware and software and the provision of certain cloud- based solutions to certain countries, governments and persons targeted by **US** ~~U. S.~~ sanctions and for certain end- uses. As an example, following Russia' s invasion of Ukraine, the **US** ~~United States~~ and other countries imposed economic sanctions and severe export control restrictions against Russia and Belarus. The **US** ~~United States~~ and its allies could expand and strengthen these sanctions and export restrictions and take other actions should the conflict further escalate. These restrictions would further impact our ability to do business in certain parts of the world and to do business with certain persons and entities, including selling our services and using local developers. We also collect information about cyber threats from open sources, intermediaries and third parties that we make available to our customers in our threat industry publications. **Further, regulators in the US and elsewhere have signaled an increased emphasis on sanctions and export control enforcement, including several recent high- profile enforcement actions and increased pressure for companies to self- disclose potential violations.** While we have implemented certain procedures to facilitate compliance with applicable laws and regulations in connection with the collection and distribution of this information, we cannot assure you that these procedures have been effective or that we, or third parties who we do not control,

have complied with all laws or regulations in this regard. Failure by our employees, representatives, contractors, channel partners, agents, intermediaries, or other third parties to comply with applicable laws and regulations in the collection and distribution of this information also could have negative consequences to us, including reputational harm, government investigations, and penalties. Although we take precautions to prevent our information collection practices and services from being provided in violation of such laws, our information collection practices and services may have been in the past, and could in the future be, provided in violation of such laws. If we or our employees, representatives, contractors, channel partners, agents, intermediaries, or other third parties fail to comply with these laws and regulations, we could be subject to civil or criminal penalties, including the possible loss of export privileges and fines. We may also be adversely affected through reputational harm, loss of access to certain markets or otherwise. Obtaining the necessary authorizations, including any required license, for a particular transaction may be time- consuming, is not guaranteed and may result in the delay or loss of sales opportunities. Various countries regulate the import of certain encryption technology, including through import permit and license requirements, and have enacted laws that could limit our ability to distribute our platform or could limit our customers' ability to implement our platform in those countries. Additionally, export restrictions ~~recently~~ imposed on Russia and Belarus specifically limit the export of encryption hardware, software and related source code and technology to these locations which could limit our ability to provide our software and services to these countries. Changes in our platform ~~or~~ **, and** changes in **or promulgation of new** export and import regulations may create delays in the introduction of our platform into international markets, prevent our customers with international operations from deploying our platform globally or, in some cases, prevent the export or import of our platform to certain countries, governments or persons altogether. Any change in export or import regulations, economic sanctions or related legislation, shift in the enforcement or scope of existing regulations, or change in the countries, governments, persons or technologies targeted by such regulations, could result in decreased use of our platform by, or in our decreased ability to export or sell our platform to, existing or potential customers with international operations. Any decreased use of our platform or limitation on our ability to export or sell our platform would adversely affect our business, operating results, and financial condition. We are also subject to the United States Foreign Corrupt Practices Act of 1977 (FCPA), as amended, the United Kingdom Bribery Act 2010 (the Bribery Act), and other anti- corruption, sanctions, anti- bribery, anti- money laundering and similar laws in the **US** ~~United States~~ and other countries in which we conduct activities. Anti- corruption and anti- bribery laws, which have been enforced aggressively and are interpreted broadly, prohibit companies and their employees, agents, intermediaries and other third parties from promising, authorizing, making or offering improper payments or other benefits to government officials and others in the public, and in certain cases, private sector. We leverage third parties, including intermediaries, agents and channel partners, to conduct our business in the **US** ~~United States~~ and abroad, to sell subscriptions to our platform and to collect information about cyber threats. We and these third parties may have direct or indirect interactions with officials and employees of government agencies or state- owned or affiliated entities and we may be held liable for the corrupt or other illegal activities of these third- party business partners and intermediaries, our employees, representatives, contractors, channel partners, agents, intermediaries and other third parties, even if we do not explicitly authorize such activities. While we have policies and procedures to address compliance with FCPA, Bribery Act and other anti- corruption, sanctions, anti- bribery, anti- money laundering and similar laws, we cannot assure you that they will be effective, or that all of our employees, representatives, contractors, channel partners, agents, intermediaries or other third parties have not taken, or will not take actions, in violation of our policies and applicable law, for which we may be ultimately held responsible. As we increase our international sales and business, including our business with government organizations, our risks under these laws may increase. Noncompliance with these laws could subject us to investigations, severe criminal or civil sanctions, settlements, prosecution, loss of export privileges, suspension or debarment from **US** ~~U. S.~~ government contracts, other enforcement actions, disgorgement of profits, significant fines, damages, other civil and criminal penalties or injunctions, whistleblower complaints, adverse media coverage and other consequences. Any investigations, actions or sanctions could harm our reputation, business, operating results, and financial condition **. Moreover, the rapid evolution of AI, including potential government regulation of AI, may require significant additional resources to develop, test, and maintain our platform. Our AI- related initiatives may result in new or enhanced governmental or regulatory scrutiny, including regarding the use of AI in our products and the marketing of products using AI, litigation, customer reporting or documentation requirements, ethical or social concerns, or other complications and may also introduce risks related to accuracy, bias, toxicity, privacy, and security and data provenance. For example, the European Commission' s proposed Artificial Intelligence Act could also impose new obligations or limitations affecting our business, if and when it enters into force** . If we fail to adequately protect personal information or other information we collect, process, share or maintain under applicable laws, our business, operating results, and financial condition could be adversely affected. We receive, store, and process ~~some~~ personal information from our employees, customers, the employees of our customers, and our end users. This personal information is hosted by our third- party service providers. A wide variety of state, national, and international laws, as well as regulations and industry standards apply to the collection, use, retention, protection, disclosure, transfer and other processing of personal information and other information, the scope of which are changing, subject to differing interpretations, and may be inconsistent across countries or conflict with other rules. Data protection and privacy- related laws and regulations are evolving and may result in ~~ever~~ increasing regulatory and public scrutiny and escalating levels of enforcement and sanctions. Failure to comply with laws, regulations and industry standards regarding personal information or other information could adversely affect our business, operating results **,** and financial condition. Complying with these various laws and regulations could cause us to incur substantial costs or require us to change our business practices, systems, and compliance procedures in a manner adverse to our business. In the **US** ~~United States~~ , there are numerous federal and state consumer, privacy **,** and data security laws and regulations governing the collection, use, disclosure, and protection of personal information, including security breach notification laws and consumer protection laws. Each of these laws is subject to varying interpretations and constantly evolving.

Notably, but not necessarily limited to, we may be subject to: • Controlling the Assault of Non- Solicited Pornography And Marketing Act (**also known as the "** CAN- SPAM **Act "**) and similar state consumer protection laws regarding the use of telephones and text messaging for marketing purposes. • Section 5 (a) of the Federal Trade Commission (FTC) Act for violating consumers' privacy rights or failing to take appropriate steps to keep consumers' personal information secure, resulting in a finding of an unfair act or practice. • The CCPA, effective since January 1, 2020, which created new data privacy obligations for covered ~~companies~~ **businesses** and provided new privacy rights to California residents, including the right to opt out of certain disclosures of their information and receive detailed information about how their personal information is used. The CCPA provides for civil penalties for violations, as well as a private right of action for data breaches that is expected to increase data breach litigation. A ballot initiative called the California Privacy Rights Act **(** ~~, or~~ CPRA ~~, took effect January 1, 2023 (with a look back to January 2022~~) **went into force** ~~, with enforcement beginning on~~ July 1, 2023, and significantly modifies the CCPA, including by expanding consumers' rights with respect to certain sensitive personal data. The CPRA also creates a new state agency, known as the California Privacy Protection Agency, **which is** ~~that will be~~ vested with **the** authority to implement and enforce the CCPA and the CPRA. Potential uncertainty surrounding the CCPA and CPRA may increase our compliance costs and potential liability, particularly in the event of a data breach, and could have a material adverse effect on our business. • Other states have ~~followed California~~ **enacted consumer privacy laws comparable to the CCPA that came into effect in 2023** : Virginia enacted the Virginia Consumer Data Protection Act **which** ~~that also~~ became effective January 1, 2023; Colorado **and Connecticut** enacted ~~its~~ **the** Colorado Privacy Act **and the Connecticut Personal Data Privacy and Online Monitoring Act** , **which both became effective July 1, 2023; Utah enacted the Utah Consumer Privacy Act, which became effective December 31, 2023. In addition, as of December 31, 2023, eight other states (Delaware, Indiana, Iowa, Florida, Montana, Oregon, Tennessee and Texas) enacted privacy legislation** which will become effective **between** July 1, ~~2023~~ **2024 and January** ~~; Connecticut passed the Connecticut Data Privacy Act (CDPA), which will become effective July~~ 1, ~~2023~~ **2026 . Numerous** ~~; and Utah enacted the~~ **other** ~~Utah Consumer Privacy Act (UCPA), which will become effective December 31, 2023; and as the year 2023 began, four~~ states ~~had~~ **also have** pending consumer privacy legislation under review, which if enacted, would add additional costs and expense of resources to maintain compliance. In certain circumstances, we may **also** be subject to the ~~EU General Data Protection Regulation (~~ GDPR ~~)~~ (established in 2018 and implemented by countries in the EEA) and the **UK** ~~U. K. General Data Protection Regulation and U. K. Data Protection Act 2018 (U. K.~~ GDPR ~~)~~ , which respectively govern the collection, use, disclosure, transfer or other processing of personal data of natural persons, and it applies extra- territorially and imposes onerous requirements on controllers and processors of personal data, including, for example: (i) accountability and transparency requirements, and enhanced requirements for obtaining valid consent; (ii) obligations to consider data protection as any new products or services are developed and to limit the amount of personal data processed; (iii) obligations to comply with data protection rights of data subjects; and (iv) reporting of personal data breaches to the supervisory authority without undue delay (and no later than 72 hours). Companies that must comply with the GDPR face increased compliance obligations and risk, including more robust regulatory enforcement of data protection requirements and potential fines for noncompliance of up to € 20 million or 4 ~~percent~~ **%** of the annual global ~~revenues~~ **turnover** of the noncompliant company, whichever is greater. Additionally, following the withdrawal by the **UK** ~~United Kingdom (U. K.)~~ from the **EU** ~~European Union~~ and the EEA, companies must comply with both the GDPR and the **UK** ~~U. K.~~ GDPR as incorporated into **UK** ~~United Kingdom~~ national law, the latter regime having the ability to separately fine up to the greater of £ 17. 5 million or 4 ~~percent~~ **%** of global **annual** turnover. In addition to the foregoing, a breach of the GDPR or **UK** ~~U. K.~~ GDPR could result in regulatory investigations, reputational damage, orders to cease or change our processing of our data, enforcement notices, and / or assessment notices (for a compulsory audit). We may also face civil claims including representative actions and other class action type litigation (where individuals have suffered harm), potentially amounting to significant compensation or damages liabilities, as well as associated costs, diversion of internal resources, and reputational harm. The GDPR and **UK** ~~U. K.~~ GDPR requires, among other things, that personal ~~information~~ **data** only be transferred outside of the EEA, or the **UK** ~~U. K.~~ , respectively to jurisdictions that have been deemed adequate (also known as " Third Countries, " ~~which at present time includes the United States~~) by the European Commission or by the **UK** ~~U. K.~~ data protection regulator, respectively. Accordingly, personal ~~information~~ **data** may not be transferred to those jurisdictions that have not been deemed adequate, unless steps are taken to legitimize those data transfers. Switzerland follows similar legal practices. **We rely** ~~Previously, we relied~~ on ~~the E. U.- U. S. Privacy Shield framework to provide a mechanism for the transfer of data from E. U. Member States to the United States, but this was invalidated by the European Court of Justice (CJEU) on July 16, 2020, on the grounds that the Privacy Shield failed to offer adequate protections to E. U. personal information transferred to the United States. We previously relied on our own, as well as our vendors', Privacy Shield certification for the purposes of transferring personal data from the EEA to the United States in compliance with the GDPR / U. K. GDPR' s data export conditions, which are no longer allowed. One such alternative to the Privacy Shield is~~ the use of Standard Contractual Clauses (SCCs), a standard form of contract approved by the European Commission **,** as an adequate personal data transfer mechanism **for the transfer of personal data to Third Countries; however** , **the SCCs** may not be alone sufficient to protect data transferred to the **US** ~~United States~~ or other Third Countries under certain circumstances without making a case- by- case basis assessment of the legal regime applicable in the destination country according to the CJEU. On June 28, 2021, the European Commission issued an adequacy decision for personal ~~information~~ **data** transfers from the EEA to the **UK** ~~U. K.~~ , with a sunset clause of four years, meaning that the European Commission will review and renew only if the European Commission considers that the **UK** ~~U. K.~~ continues to ensure an adequate level of data protection. Notably, the European Commission reserved a right to intervene at any time during the four- year adequacy period if the **UK** ~~U. K.~~ deviates from the level of protection then in place. If this adequacy decision is reversed by the European Commission, we would have to implement protection measures such as the SCCs for **personal** data transfers between the **EU** ~~E. U.~~ and the **UK** ~~U. K.~~ or find alternative solutions for the compliant transfer of personal data from the **EU** ~~E. U.~~ into the ~~U~~ **UK In March 2022, the UK**

Information Commissioner' s Office adopted an International Data Transfer Agreement (IDTA) for transfers of personal data out of the UK to so- called third countries, as well as an international data transfer addendum (UK SCC Addendum) that can be used with the SCCs for the same purpose . ~~K~~ **To add to this complexity, effective on July 10, 2023, the European Commission adopted the new EU- US Data Privacy Framework (DPF) which allows for transfers of personal data from the EU to certified companies in the US without the need for additional privacy safeguards as an alternative to the SCCs. In October 2023, a UK extension to the DPF (the UK – US Data Bridge) was adopted enabling the transfer of personal data between the UK and US entities without the need for an IDTA or UK SCC Addendum. However, the DPF and the UK – US Data Bridge could be subject to further legal challenge which could cause the legal requirements for personal data transfers from the EU and the UK to the US to become uncertain once again** . Some countries (including some outside the EEA) also are considering or have passed legislation requiring local storage and processing of data, or similar requirements, which could increase the cost and complexity of delivering our products and services if we were to operate in those countries. If we are required to implement additional measures to transfer data from the EEA, this could increase our compliance costs, and could adversely affect our business, financial condition and results of operations. The myriad **of** international and **US** ~~U. S.~~ privacy and data breach laws are not consistent, and compliance in the event of a widespread data breach is difficult and may be costly. In many jurisdictions, enforcement actions and consequences for noncompliance are also rising. In addition to government regulation, privacy advocates and industry groups may propose new and different self- regulatory standards that either legally or contractually apply to us. As supervisory authorities continue to issue further guidance on personal information transfers (including regarding data export and circumstances in which we cannot use the SCCs), we could suffer additional costs, complaints, or regulatory investigations or fines. If we are otherwise unable to transfer personal data between and among countries and regions in which we operate, it could affect the manner in which we provide our services, adversely affecting our financial results, and possibly making it necessary to establish **localized storage** systems in the EEA, Switzerland, and the **UK** ~~U. K.~~ to maintain personal data originating from those jurisdictions that adds expenses and may create distractions from our other business pursuits. Loss, retention or misuse of certain information and alleged violations of laws and regulations relating to privacy and data security, and any relevant claims, may expose us to potential liability and may require us to expend significant resources on data security and in responding to and defending such allegations and claims. We are also subject to evolving **EU** ~~E. U.~~ and **UK** ~~U. K.~~ privacy laws on cookies and electronic marketing. In the **EU** ~~E. U.~~ and the **UK** ~~U. K.~~ , informed opt- in consent is required for the placement of a cookie or similar technologies on a user' s device and for direct electronic marketing. The GDPR also imposes conditions on obtaining valid consent, such as a prohibition on pre- checked consents and a requirement to ensure separate consents are sought for each type of cookie or similar technology. While we anticipate the development of the ePrivacy Regulation to govern cookies and e- marketing, recent European court decisions and regulators' guidance are driving increased attention to cookies and tracking technologies. If regulators start to enforce the strict approach in recent guidance, this could lead to substantial costs, require significant systems changes, limit the effectiveness of our marketing activities, divert the attention of our technology personnel, adversely affect our margins, increase costs and subject us to additional liabilities. Regulation of cookies and similar technologies, and any decline of cookies or similar online tracking technologies as a means to identify and potentially target users, may lead to broader restrictions and impairments on our marketing and personalization activities and may negatively impact our efforts to understand users. Similar concerns may happen under the new CPRA regime in California **and other current and soon- to- be enacted US state privacy laws** . Additionally, by expanding into the **EU** ~~E. U.~~ and **UK** ~~U. K.~~ , we may also trigger Article 3 (2) of the GDPR / **UK** ~~U. K.~~ GDPR directly as we may be considered to be monitoring data subjects. To the extent we process personal data on behalf of our customers for the provision of services, we have, and may in the future, also be required to enter into data processing agreements which comply with Article 28 of the GDPR / **UK** ~~U. K.~~ GDPR. We depend on a number of third parties in relation to the operation of our business, a number of which process personal data on our behalf or as our sub- processor. To the extent required by applicable law, we attempt to mitigate the associated risks of using third parties by performing security assessments and detailed due diligence, entering into contractual arrangements to ensure that providers only process personal data according to our instructions or comparable instructions to the instructions of our customer (as applicable), and that they have sufficient technical and organizational security measures in place. There is no assurance that these contractual measures and our own privacy and security- related safeguards will protect us from the risks associated with the third- party processing, storage and transmission of such information. Any violation of **privacy,** data **protection, data** or ~~security~~ **cybersecurity** laws by our third- party processors could have a material adverse effect on our business and result in the fines and penalties under the GDPR and the **UK** ~~U. K.~~ GDPR outlined above. In recent years, some regulators have proposed or introduced cybersecurity licensing requirements or certification regimes for specific sectors, such as critical infrastructure. These may impose new requirements on us or our current or prospective customer including, but not limited to, data processing locations, breach notification, and security standards. Such requirements may cause us to incur significant organizational costs and increase barriers of entry into new markets. New worldwide data protection laws, including **in** the **US** ~~U. S.~~ and European jurisdictions described above, may lead to ~~ever~~ changing definitions of personal information and other sensitive information which may also limit or inhibit our ability to operate or expand our business, including limiting strategic partnerships that may involve the sharing of data. Notably some foreign jurisdictions require that certain types of data be retained on servers within these respective jurisdictions. Our failure to comply with applicable laws, directives, and regulations may result in enforcement action against us, including fines, and damage to our reputation, any of which may have an adverse effect on our business and operating results. Any failure or perceived failure by us, even if unfounded, to comply with applicable privacy and data security laws and regulations, our privacy policies, or our privacy- related obligations to customers, users or other third parties, or any compromise of security that results in the unauthorized release or transfer of personal information or other customer data, may result in governmental enforcement actions, **fines, penalties,** litigation, or

public statements against us by consumer advocacy groups or others and could cause our users to lose trust in us, which would have an adverse effect on our reputation and business. For example, in 2017, we reached a consent agreement with the FTC, to resolve an investigation relating to certain disclosures in our privacy policy. The consent agreement requires us, among other things, to provide information **to the FTC** about our compliance with the FTC order and about representations made in our marketing materials. We may be subject to future investigations and legal proceedings by the FTC or other regulators. ~~A~~ **As** such, it is possible that a regulatory inquiry might result in changes to our policies or business practices. Violation of existing or future regulatory orders or consent decrees could subject us to substantial monetary fines and other penalties that could negatively affect our operating results and financial condition. In addition, it is possible that future orders issued by, or enforcement actions initiated by, regulatory authorities could cause us to incur substantial costs or require us to change our business practices in a manner materially adverse to our business. Any significant change to applicable laws, regulations or industry practices regarding the use or disclosure of our customers' data, or regarding the manner in which the express or implied consent of customers for the use and disclosure of such data is obtained – or in how these applicable laws, regulations or industry practices are interpreted and enforced by state, federal and international privacy regulators – could require us to modify our services and features, possibly in a material manner, may subject us to regulatory enforcement actions and fines, and may limit our ability to develop new products, services and features that make use of the data that our customers voluntarily share with us. Any security breach or incident, including those resulting from a cybersecurity attack, phishing attack, unauthorized access, unauthorized usage, virus, malware, ransomware, denial of service, credential stuffing attack, supply chain attack, hacking or similar breach involving our networks and systems, or those of third parties upon which we rely, could result in the loss of customer data, including personal information, disruption to our operations, significant remediation costs, lost revenue, increased insurance premiums, damage to our reputation, litigation, regulatory investigations, or other liabilities. These attacks may come from individual hackers, criminal groups, and state- sponsored organizations, and security breaches and incidents may arise from other sources, such as employee or contractor error or malfeasance. Cyber threats are evolving and becoming increasingly sophisticated and complex, increasing the difficulty of detecting and successfully defending against them. As a cybersecurity company, we have been and may continue to be specifically targeted by ~~bad~~ **malicious** actors for attacks intended to circumvent our security capabilities as an entry point into customers' endpoints, networks, or systems. Our industry is experiencing an increase in phishing attacks and unauthorized scans of systems searching for vulnerabilities or misconfigurations to exploit. If our security measures are breached or otherwise compromised as a result of third- party action, employee or contractor error, defect, vulnerability or bug in our products or products of third parties upon which we rely, malfeasance or otherwise, including any such breach or compromise resulting in someone obtaining unauthorized access to our confidential information, including personal information or the personal information of our customers or others, or if any of these are perceived or reported to occur, we may suffer the loss, compromise, corruption, unavailability, or destruction of our or others' confidential information and personal information, we may face a loss in intellectual property protection, our reputation may be damaged, our business may suffer and we could be subject to claims, demands, regulatory investigations and other proceedings, indemnity obligations, and otherwise incur significant liability. Even the perception of inadequate security may damage our reputation and negatively impact our ability to win new customers and retain existing customers. Further, we could be required to expend significant capital and other resources to address any security incident or breach, and we may face difficulties or delays in identifying and responding to any security breach or incident. Techniques used to sabotage or obtain unauthorized access to systems or networks are constantly evolving and, in some instances, are not identified until launched against a target. We and our third- party vendors and service providers may be unable to anticipate these techniques, react in a timely manner, or implement adequate preventative measures. Due to political uncertainty and military actions associated with **the conflicts in** ~~Russia's invasion of~~ Ukraine **, the Middle East and tensions between China and Taiwan** , we and our third-party vendors and service providers are vulnerable to a heightened risk of cybersecurity attacks, phishing attacks, viruses, malware, ransomware, hacking or similar breaches from nation- state and affiliated actors, including attacks that could materially disrupt our **and our third- party vendors' and service providers'** systems and operations, supply chain, and ability to produce, sell and distribute our products and services as well as retaliatory cybersecurity attacks from Russian and Russian-affiliated actors against companies with a **US** ~~U. S.~~ presence. In addition, laws, regulations, government guidance, and industry standards and practices in the **US** ~~United States~~ and elsewhere are rapidly evolving to combat these threats. We may face increased compliance burdens regarding such requirements with regulators and customers regarding our products and services and also incur additional costs for oversight and monitoring of our own supply chain. We and our customers may also experience increased costs associated with security measures and increased risk of suffering cyberattacks, including ransomware attacks. Should we or the third- party vendors and service providers upon which we rely experience such attacks, including from ransomware or other security breaches or incidents, our operations may also be hindered or interrupted due to system disruptions or otherwise, with foreseeable secondary contractual, regulatory, financial and reputational harms that may arise from such an incident. Further, we cannot assure that any limitations of liability provisions in our customer agreements, contracts with third-party vendors and service providers or other contracts would be enforceable or adequate or would otherwise protect us from any liabilities or damages with respect to any particular claim relating to a security breach or other security incident. We also cannot be sure that our existing insurance coverage will continue to be available on acceptable terms or will be available in sufficient amounts to cover claims related to a security incident or breach, or that the insurer will not deny coverage as to any future claim. The successful assertion of claims against us that exceed available insurance coverage, or the occurrence of changes in our insurance policies, including premium increases or the imposition of large deductible or coinsurance requirements, could have a material adverse effect on our business, including our financial condition, operating results, and reputation. **Moreover, while we strive to publish and prominently display privacy policies that are accurate, comprehensive, and compliant with applicable laws, rules regulations and industry standards, we cannot ensure that our privacy policies and other**

statements regarding our practices will be sufficient to protect us from claims, proceedings, liability or adverse publicity relating to data privacy and security. If our public statements about our use, collection, disclosure and other processing of personal information, whether made through our privacy policies, information provided on our website, press statements or otherwise, are alleged to be deceptive, unfair or misrepresentative of our actual practices, we may be subject to potential government or legal investigation or action, including by the FTC or applicable state attorneys general. Our compliance efforts are further complicated by the fact that data privacy and security laws, rules, regulations and standards around the world are rapidly evolving, may be subject to uncertain or inconsistent interpretations and enforcement, and may conflict among various jurisdictions. Any failure or perceived failure by us to comply with our privacy policies, or applicable data privacy and security laws, rules, regulations, standards, certifications or contractual obligations, or any compromise of security that results in unauthorized access to, or unauthorized loss, destruction, use, modification, acquisition, disclosure, release or transfer of personal information, may result in requirements to modify or cease certain operations or practices, the expenditure of substantial costs, time and other resources, proceedings or actions against us, legal liability, governmental investigations, enforcement actions, claims, fines, judgments, awards, penalties, sanctions, and costly litigation (including class actions). Any of the foregoing could harm our reputation, distract our management and technical personnel, increase our costs of doing business, adversely affect the demand for our products and services, and ultimately result in the imposition of liability, any of which could have a material adverse effect on our business, operating results, and financial condition. We **are currently in, and** may **in the future,** become involved in litigation that may adversely affect us. From time to time, we have been subject to claims, suits and other proceedings. For example, we are currently the subject of **securities** litigation ~~with BlackBerry Corp~~ **and commercial litigation** . For additional information regarding ~~this~~ **these** litigation **matters** , see the section titled " ~~Part I — Legal Proceedings.~~ " Regardless of the outcome, legal proceedings can have an adverse impact on us because of legal costs and diversion of management attention and resources, and could cause us to incur significant expenses or liability, adversely affect our brand recognition or require us to change our business practices. The expense of litigation and the timing of this expense from period to period are difficult to estimate, subject to change and could adversely affect our business, operating results **,** and financial condition. It is possible that a resolution of one or more such proceedings could result in substantial damages, settlement costs, fines and penalties that would adversely affect our business, consolidated financial condition, operating results or cash flows in a particular period. These proceedings could also result in reputational harm, sanctions, consent decrees or orders requiring a change in our business practices. Because of the potential risks, expenses and uncertainties of litigation, we may, from time to time, settle disputes, even where we have meritorious claims or defenses, by agreeing to settlement agreements. Because litigation is inherently unpredictable, we cannot assure you that the results of any of these actions will not have a material adverse effect on our business, operating results, financial condition, and prospects. Any of these consequences could adversely affect our business, operating results, and financial condition. Risks Related to Financial and Accounting Matters The requirements of being a public company, including maintaining adequate internal control over our financial and management systems, result in significant costs and may strain our resources, divert management' s attention, and affect our ability to attract and retain executive management and qualified board members. As a public company we incur **and expect to continue to incur** significant legal, accounting, and other expenses. We are subject to the reporting requirements of the Exchange Act, the Sarbanes- Oxley Act, Dodd- Frank Wall Street Reform and Consumer Protection Act of 2010 and the rules and regulations of the applicable listing standards of the New York Stock Exchange (NYSE). We expect that the requirements of these rules and regulations will continue to increase our legal, accounting, and financial compliance costs, make some activities more difficult, time- consuming, and costly, and place significant strain on our personnel, systems, and resources. The Sarbanes-Oxley Act requires, among other things, that we maintain effective disclosure controls and procedures and internal control over financial reporting. We are continuing to develop and refine our disclosure controls, internal control over financial reporting and other procedures that are designed to ensure information required to be disclosed by us in our **consolidated** financial statements and in the reports that we will file with the SEC is recorded, processed, summarized and reported within the time periods specified in SEC rules and forms, and information required to be disclosed in reports under the Exchange Act is accumulated and communicated to our principal executive and financial officers. Our current controls and any new controls we develop may become inadequate because of changes in conditions in our business. Additionally, to the extent we acquire other businesses, the acquired companies may not have a sufficiently robust system of internal controls and we may uncover new deficiencies. Further, weaknesses in our internal controls may be discovered in the future. Any failure to develop or maintain effective controls, or any difficulties encountered in their implementation or improvement, could harm our operating results, may result in a restatement of our **consolidated** financial statements for prior periods, cause us to fail to meet our reporting obligations, and could adversely affect the results of periodic management evaluations and annual independent registered public accounting firm attestation reports regarding the effectiveness of our internal control over financial reporting ~~that we are required to include in our annual reports on Form 10- K filed with the SEC beginning in fiscal year 2023~~ . Ineffective disclosure controls and procedures and internal control over financial reporting could also cause investors to lose confidence in our reported financial and other information, which would likely have a negative effect on the market price of our Class A common stock. Our management is also required, pursuant to Section 404 of the Sarbanes- Oxley Act, to certify financial and other information in our quarterly and annual reports and provide an annual report on the effectiveness of our internal control over financial reporting. In addition, changing laws, regulations, and standards relating to corporate governance and public disclosure, including those related to climate change and other **environmental, social, and governance (** ESG **)** - focused disclosures, are creating uncertainty for public companies, increasing legal and financial compliance costs, and making some activities more time consuming. These laws, regulations, and standards are subject to varying interpretations, in many cases due to their lack of specificity, and, as a result, their application in practice may evolve over time as new guidance is provided by regulatory and

governing bodies. This could result in continuing uncertainty regarding compliance matters and higher costs necessitated by ongoing revisions to disclosure and governance practices. We intend to continue to invest resources to comply with evolving laws, regulations, and standards, and this investment may result in increased general and administrative expenses and a diversion of management' s time and attention from revenue- generating activities to compliance activities. If our efforts to comply with new laws, regulations, and standards differ from the activities intended by regulatory or governing bodies due to ambiguities related to their application and practice, regulatory authorities may initiate legal proceedings against us, and our business may be adversely affected. We have incurred significant costs with respect to our directors' and officers' insurance coverage. In the future, it may be more expensive or more difficult for us to obtain director and officer liability insurance, and we may be required to accept reduced coverage or incur substantially higher costs to obtain coverage. These factors would also make it more difficult for us to attract and retain qualified members of our board of directors, particularly to serve on our audit committee and compensation committee, and qualified executive officers. Being a public company requires significant resources and management oversight. As a result, management' s attention may be diverted from other business concerns, which could harm our business, operating results, and financial condition. We could be subject to additional tax liabilities and **US** ~~United States~~ federal and global income tax reform could adversely affect us. We are subject to **US** ~~U. S.~~ federal, state, local and sales taxes in the **US** ~~United States~~ and foreign income taxes, withholding taxes and transaction taxes in numerous foreign jurisdictions. Significant judgment is required in evaluating our tax positions and our worldwide provision for income taxes. During the ordinary course of business, there are many activities and transactions for which the ultimate tax determination is uncertain. In addition, our future income tax obligations could be adversely affected by changes in, or interpretations of, tax laws in the **US** ~~United States~~ or in other jurisdictions in which we operate. For example, the **US** ~~United States~~ tax law legislation **,** commonly referred to as the Tax Cuts and Jobs Act of 2017 ~~(the Tax Act) (as modified by the Coronavirus Aid, Relief, Economic Security Act, the Families First Coronavirus Response Act and the American Rescue Plan Act)~~ , significantly reformed the Internal Revenue Code of 1986, as amended (~~or~~ the Internal Revenue Code), reducing **US** ~~U. S.~~ federal tax rates, making sweeping changes to rules governing international business operations, and imposing significant additional limitations on tax benefits, including the deductibility of interest and the use of net operating loss carryforwards. On August 16, 2022, President Biden signed the Inflation Reduction Act of 2022 (IRA) into law. The IRA contains certain tax measures, including a corporate alternative minimum tax of 15 % on some large corporations and an excise tax of 1 % on certain corporate stock buy-backs taking place after December 31, 2022. ~~We are currently evaluating the various provisions of the IRA and currently anticipate that its impact, if any, will not be material to our operating results or cash flows. In the United States, Congress and the Biden administration continue to consider other proposed legislation to make various tax law changes. These proposals, could include changes to the existing framework in respect of income taxes, limitations on the ability of taxpayers to claim and utilize foreign tax credits, as well as add new types of non- income taxes (such as taxes based on a percentage of revenue or taxes applicable to digital services).~~ In addition, the Organization for Economic Cooperation and Development (OECD) Inclusive Framework of 137 jurisdictions have joined a two- pillar plan to reform international taxation rules. The first pillar is focused on the allocation of taxing rights between countries for in- scope multinational enterprises that sell goods and services into countries with little or no local physical presence and is intended to apply to multinational enterprises with global turnover above **€** 20 billion ~~euros~~ . The second pillar is focused on developing a global minimum tax rate of at least 15 percent applicable to in- scope multinational enterprises and is intended to apply to multinational enterprises with annual consolidated group revenue in excess of **€** 750 million ~~euro~~ . ~~While substantial work remains~~ **We are still evaluating the impact of the pillar two rules as they continue** to be ~~completed~~ **refined** by the OECD and **implemented by various** national governments ~~on the implementation of~~ **. However, it is possible that** ~~these~~ -- **the pillar** ~~proposals, future tax reform resulting from these developments may result in changes to~~ **two rules** ~~long- standing tax principles~~ , ~~which~~ **as implemented by various national governments,** could adversely affect our effective tax rate or result in higher cash tax liabilities. Due to the large and expanding scale of our international business activities, these types of changes to the taxation of our activities could impact the tax treatment of our foreign earnings, increase our worldwide effective tax rate, increase the amount of taxes imposed on our business, and harm our financial position. Such changes may also apply retroactively to our historical operations and result in taxes greater than the amounts estimated and recorded in our financial statements. Our ability to use our net operating loss carryforwards and certain other tax attributes may be limited. As of January 31, ~~2023~~ **2024** , we had aggregate **US** ~~U. S.~~ federal and state net operating loss carryforwards of $ ~~651~~ **721** . ~~1~~ **2** million and $ ~~338~~ **390** . ~~3~~ **6** million, respectively, which may be available to offset future taxable income for **US** ~~U. S.~~ income tax purposes. If not utilized, the federal net operating loss carryforwards will begin to expire in 2031, and the state net operating loss carryforwards will begin to expire in ~~2024~~ **2025** . In addition, as of January 31, ~~2023~~ **2024** , we had federal research and development credit carryforwards of $ ~~2~~ **5** . ~~0~~ **9** million, which will begin to expire in 2037, and state research and development credit carryforwards of $ 2. ~~0~~ **9** million, which do not expire. We also had foreign net operating loss carryforwards of $ ~~289~~ **202** . 8 million, as of January 31, ~~2023~~ **2024** , which do not expire. Realization of these net operating loss and research and development credit carryforwards depends on future income, and there is a risk that certain of our existing carryforwards could expire unused and be unavailable to offset future income tax liabilities, which could adversely affect our operating results and financial condition. In addition, under Sections 382 and 383 of the Internal Revenue Code, if a corporation undergoes an " ownership change, " generally defined as a greater than 50 % change (by value) in ownership by " 5 percent shareholders " over a rolling three- year period, the corporation' s ability to use its pre-change net operating loss carryovers and other pre- change tax attributes, such as research and development credits, to offset its post- change income or taxes may be limited. Similar rules apply under **US** ~~U. S.~~ state tax laws. We have, and may in the future, experience ownership changes as a result of shifts in our stock ownership. As a result, if we earn net taxable income, our ability to use our pre- change **US** ~~U. S.~~ net operating loss carryforwards to offset **US** ~~U. S.~~ federal taxable income may be subject to limitations, which could potentially result in increased future tax liability to us. We could be required to collect additional sales,

use, value added, digital services, or other similar taxes or be subject to other liabilities with respect to past or future sales, that may increase the costs our customers would have to pay for our solutions and adversely affect our business, operating results, and financial condition. We do not collect sales and use, value added, or similar taxes in all jurisdictions in which we have sales because we have been advised that such taxes are not applicable to our services in certain jurisdictions. Sales and use, value added, and similar tax laws and rates vary greatly by jurisdiction. Certain jurisdictions in which we do not collect such taxes may seek to impose incremental or new sales, use, value added, digital services, or assert other tax collection obligations on us that such taxes are applicable, which could result in tax assessments, penalties and interest, to us or our customers for the past amounts, and we may be required to collect such taxes in the future. If we are unsuccessful in collecting such taxes from our customers, we could be held liable for such costs, which may adversely affect our results of operations. Further, an increasing number of **US** ~~U. S.~~ states have considered or adopted laws that attempt to impose tax collection obligations on out- of- state companies. A successful assertion by one or more **US** ~~U. S.~~ states requiring us to collect taxes where we presently do not do so, or to collect more taxes in a jurisdiction in which we currently do collect some taxes, could result in substantial liabilities, including taxes on past sales, as well as interest and penalties. Furthermore, certain jurisdictions, such as the **UK,** ~~U. K. and~~ France **and Canada** , have **enacted** ~~recently introduced~~ a digital services tax, which is generally a tax on gross revenue generated from users or customers located in in those jurisdictions, and other jurisdictions ~~have enacted or~~ are considering enacting similar laws. A successful assertion by a **US** ~~U. S.~~ state or local government, or other country or jurisdiction that we should have been or should be collecting additional sales, use, value added, digital services or other similar taxes could, among other things, result in substantial tax payments, create significant administrative burdens for us, discourage potential customers from subscribing to our platform due to the incremental cost of any such sales or other related taxes, or otherwise harm our business. Our corporate 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 operating results and financial condition. We are expanding our international operations and staff to support our business and growth in international markets. 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 corporate structure and associated transfer pricing policies contemplate future growth in international markets, and consider the functions, risks, and assets of the various entities involved in intercompany transactions ~~. The amount of taxes we pay in different jurisdictions will depend on the application of the tax laws of the various jurisdictions, including the United States, to our intercompany transactions, international business activities, and our ability to operate our business in a manner consistent with our corporate structure and intercompany arrangements~~ . Furthermore, increases in tax rates, new or revised tax laws, and new interpretations of existing tax laws and policies by taxing authorities and courts in various jurisdictions, could result in an increase in our overall tax obligations which could adversely affect our business. Our intercompany relationships and intercompany transactions are subject to complex transfer pricing rules administered by taxing authorities in various jurisdictions in which we operate with potentially divergent tax laws. The amount of taxes we pay in different jurisdictions will depend on the application of the tax laws of the various jurisdictions, including the **US** ~~United States~~ , to our intercompany transactions, international business activities, changes in tax rates, new or revised tax laws or interpretations of existing tax laws and policies by taxing authorities and courts in various jurisdictions, and our ability to operate our business in a manner consistent with our corporate structure and intercompany arrangements. It is not uncommon for tax authorities in different countries to have conflicting views, for instance, with respect to, among other things, the manner in which the arm' s length standard is applied for transfer pricing purposes, the transfer pricing and charges for intercompany services and other intercompany transactions, or with respect to the valuation of our intellectual property and the manner in which our intellectual property is utilized within our group. In 2022, we began negotiating a bilateral Advance Pricing Agreement (APA) with the **US** ~~United States~~ and the Israeli governments, covering various transfer pricing matters for intercompany transactions relating to the intergroup utilization of our intellectual property among our group enterprises. An APA, if obtained, will provide us with a more predictable future business operating model, and preclude the relevant tax authorities from making certain transfer pricing adjustments within the scope of these agreements. These transfer pricing matters may be significant to our consolidated financial statements. If taxing authorities in any of the jurisdictions in which we conduct our international operations were to successfully challenge our transfer pricing, we could be required to reallocate part or all of our income to reflect transfer pricing adjustments, which could result in an increased tax liability to us. In such circumstances, if the country from where the income was reallocated did not agree to the reallocation, we could become subject to tax on the same income in both countries, resulting in double taxation. Furthermore, the relevant taxing authorities may disagree with our determinations as to the income and expenses attributable to specific jurisdictions. We believe that our tax and financial accounting positions are reasonable and our tax reserves are adequate to cover any potential liability. We also believe that our assumptions, judgements, and estimates are reasonable and that our transfer pricing for these intercompany transactions are on arm' s- length terms. However, the relevant tax authorities may disagree with our tax positions, including any assumptions, judgements or estimates used for these transfer pricing matters and intercompany transactions. If any of these tax authorities determine that our transfer pricing for these intercompany transactions do not meet arm' s- length criteria, and were successful in challenging our positions, we could be required to pay additional taxes, interest and penalties related thereto, which could be in excess of any reserves established ~~therefor~~ **therefore** , and which could result in higher effective tax rates, reduced cash flows **,** and lower overall profitability of our operations. Our financial statements could fail to reflect adequate reserves to cover such a contingency. We may be audited in various jurisdictions, including in jurisdictions in which we are not currently filing, and such jurisdictions may assess new or additional taxes, sales taxes and value added taxes against us. Although we believe our tax estimates are reasonable, the final determination of any tax audits or litigation could be materially different from our historical tax provisions and accruals, which could have an adverse effect on our operating results or cash flows in the period or periods for which a determination is made. If our estimates or judgments relating

to our critical accounting policies prove to be incorrect or financial reporting standards or interpretations change, our operating results could be adversely affected. The preparation of financial statements in conformity with **generally accepted accounting principles (** GAAP **)** requires management to make estimates and assumptions that affect the amounts reported in our consolidated financial statements and accompanying notes. We base our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, as discussed in the section titled " Management' s Discussion and Analysis of Financial Condition and Results of Operations. " The results of these estimates form the basis for making judgments about the carrying values of assets, liabilities and equity, and the amount of revenue and expenses that are not readily apparent from other sources. Significant assumptions and estimates used in preparing our consolidated financial statements include but are not limited to those related to stock- based compensation, the period of benefit for deferred contract acquisition costs, ~~standalone selling prices for each performance obligation,~~ useful lives of long- lived assets **and intangibles** , the ~~incremental borrowing rate used for operating lease liabilities~~ **valuation of intangibles acquired as part of a business combination** , and accounting for income taxes. Our operating results may be adversely affected if our assumptions change or if actual circumstances differ from those in our assumptions, which could cause our operating results to fall below the expectations of industry or financial analysts and investors, resulting in a potential decline in the market price of our Class A common stock. Additionally, we regularly monitor our compliance with applicable financial reporting standards and review new pronouncements and drafts thereof that are relevant to us. As a result of new standards, changes to existing standards and changes in their interpretation, we might be required to change our accounting policies, alter our operational policies and implement new or enhance existing systems so that they reflect new or amended financial reporting standards, or we may be required to restate our published financial statements. For example, SEC proposals on climate- related disclosures may require us to update our accounting or operational policies, processes, or systems to reflect new or amended financial reporting standards. Such changes to existing standards or changes in their interpretation may have an adverse effect on our reputation, business, financial condition and profit, or cause an adverse deviation from our revenue and operating profit target, which may adversely affect our financial results. We are exposed to fluctuations in currency exchange rates, which could negatively affect our business, operating results, and financial condition. Our sales contracts are denominated in **US** ~~U. S.~~ dollars, and therefore our revenue is not subject to foreign currency risk. However, strengthening of the **US** ~~U. S.~~ dollar increases the real cost of our platform to our customers outside of the **US** ~~United States~~ , which could lead to delays in the purchase of our platform and the lengthening of our sales cycle. If the **US** ~~U. S.~~ dollar continues to strengthen, this could adversely affect our operating results and financial condition. In addition, increased international sales in the future, including through continued international expansion, our channel partners and other partnerships, could result in foreign currency denominated sales, which would increase our foreign currency risk. Our operating expenses incurred outside the **US** ~~U. S.~~ and denominated in foreign currencies are increasing and are subject to fluctuations due to changes in foreign currency exchange rates. These expenses are denominated in foreign currencies and are subject to fluctuations due to changes in foreign currency exchange rates. We do not currently hedge against the risks associated with currency fluctuations but may do so, or use other derivative instruments, in the future. We may require additional capital to fund our business and support our growth, and any inability to generate or obtain such capital may adversely affect our operating results and financial condition. In order to support our growth and respond to business challenges, such as developing new features or enhancements to our platform to stay competitive, acquiring new technologies, and improving our infrastructure, we have made significant financial investments in our business and we intend to continue to make such investments. As a result, we may need to engage in additional equity or debt financings to provide the funds required for these investments and other business endeavors. If we raise additional funds through equity or convertible debt issuances, our existing stockholders may suffer significant dilution and these securities could have rights, preferences, and privileges that are superior to those of holders of our Class A common stock. We expect that our existing cash and cash equivalents will be sufficient to meet our anticipated cash needs for working capital and capital expenditures for at least the next 12 months. If we obtain additional funds through debt financing, we may not be able to obtain such financing on terms favorable to us **. Further, the current global macroeconomic environment may make it more difficult to raise additional capital on favorable terms, it at all** . Such terms may involve restrictive covenants making it difficult to engage in capital raising activities and pursue business opportunities, including potential acquisitions. The trading prices of technology companies have been highly volatile as a result of the ~~continuing effects of the COVID- 19 pandemic, the~~ conflict in **the Middle East,** Ukraine **and tensions between China and Taiwan** , inflation, ~~rising~~ interest ~~rates~~ **rate volatility** , **actual or perceived** instability in the banking system, and market downturns, which may reduce our ability to access capital on favorable terms or at all. In addition, a recession, depression, or other sustained adverse market event could adversely affect our business and the value of our Class A common stock. If we are unable to obtain adequate financing or financing on terms satisfactory to us when we require it, our ability to continue to support our business growth and to respond to business challenges could be significantly impaired and our business may be adversely affected, requiring us to delay, reduce, or eliminate some or all of our operations. Our Class A common stock price is likely to continue to be volatile and could be subject to wide fluctuations. The market price of our Class A common stock depends on a number of factors, including those described in this " Risk Factors " section, many of which are beyond our control and may not be related to our operating performance. These fluctuations could cause you to lose all or part of your investment in our Class A common stock. Factors that could cause fluctuations in the market price of our Class A common stock include the following: • actual or anticipated changes or fluctuations in our operating results; • the financial projections we may provide to the public, any changes in these projections or our failure to meet these projections; • announcements by us or our competitors of new products or new or terminated significant contracts, commercial relationships, acquisitions or capital commitments; • rumors and market speculation involving us or other companies in our industry; • the overall performance of the stock market or technology companies; • the number of shares of our Class A common stock publicly owned and available for trading; • failure of industry or financial analysts to maintain coverage of us, changes in financial

estimates by any analysts who follow our company, or our failure to meet these estimates or the expectations of investors; • litigation or other proceedings involving us, our industry or both, or investigations by regulators into our operations or those of our competitors; • developments or disputes concerning our intellectual property rights or our solutions, or third- party proprietary rights; • new laws or regulations or new interpretations of existing laws or regulations applicable to our business; • any major changes in our management or our board of directors; • **the global political, economic and macroeconomic climate, including but not limited to, actual or perceived instability in the banking industry, potential uncertainty with respect to the federal debt ceiling and budget and potential government shutdowns related thereto, labor shortages, supply chain disruptions, potential recession, inflation, and rising** interest ~~rate~~ **rates** ~~changes or fluctuations~~ ; ~~and~~ • other events or factors, including those resulting from ~~the COVID- 19 pandemic,~~ war ~~, such as Russia' s invasion of Ukraine~~ , armed conflict, **including the conflicts in the Middle East, Ukraine and tensions between China and Taiwan,** incidents of terrorism or responses to these events **; and • cybersecurity incidents** . In addition, the stock market in general, and the market for technology companies in particular, has experienced extreme price and volume fluctuations that have often been unrelated or disproportionate to the operating performance of those companies, particularly during the current period of **global** macroeconomic uncertainty, including rising inflation, increasing interest rates, labor shortages and fluctuations in international currency rates, as well as the impacts of ~~the current~~ **regional geopolitical** ~~conflict~~ **conflicts , including the conflicts** in **the Middle East,** Ukraine and ~~the COVID- 19 pandemic~~ **tensions between China and Taiwan** . These economic, political, regulatory and market conditions have and may continue to negatively impact the market price of our Class A common stock, regardless of our actual operating performance. In addition, in the past, following periods of volatility in the overall market and the market prices of a particular company' s securities, securities class action litigation has often been instituted against that company. Securities litigation, if instituted against us, could result in substantial costs and divert our management' s attention and resources from our business. This could have an adverse effect on our business, operating results, and financial condition. Sales of substantial amounts of our Class A common stock in the public markets, or the perception that they might occur, could cause the market price of our Class A common stock to decline. Sales of a substantial number of shares of our Class A common stock into the public market, including shares of Class A common stock held by our existing stockholders that have been converted from shares of Class B common stock, and particularly sales by our directors, executive officers, and principal stockholders, or the perception that these sales might occur, could cause the market price of our Class A common stock to decline. In addition, pursuant to our amended and restated investors' rights agreement, dated October 28, 2020, certain stockholders have the right, subject to certain conditions, to require us to file a registration statement for the public resale of such capital stock or to include such shares in registration statements that we may file for us or other stockholders. Any registration statement we file to register additional shares, whether as a result of registration rights or otherwise, could cause the market price of our Class A common stock to decline or be volatile. We may also issue our shares of our capital stock or securities convertible into shares of our capital stock from time to time in connection with a financing, an acquisition, an investment, or otherwise. Any such issuance could result in substantial dilution to our existing stockholders and cause the market price of our Class A common stock to decline. The dual class structure of our common stock has the effect of concentrating voting control with the holders of our Class B common stock who held, in the aggregate, approximately ~~85~~ **72** % of the voting power of our capital stock as of January 31, ~~2023~~ **2024** , which will limit or preclude your ability to influence corporate matters, including the election of directors and the approval of any change of control transaction. Our Class B common stock has 20 votes per share, and our Class A common stock has one vote per share. As of January 31, ~~2023~~ **2024** , the holders of our outstanding Class B common stock held approximately ~~85~~ **72** % of the voting power of our outstanding capital stock. Because of the twenty- to- one voting ratio between our Class B and Class A common stock, the holders of our Class B common stock collectively are expected to continue to control a majority of the combined voting power of our common stock and therefore will be able to control all matters submitted to our stockholders for approval until the earlier of (i) the date specified by a vote of the holders of 66 2 / 3 % of the then outstanding shares of Class B common stock, (ii) seven years from the date of our **prospectus filed with the SEC pursuant to Rule 424 (b) (4) under the Securities Act (the** Final Prospectus **)** , or June 29, 2028, (iii) the first date following the completion of our IPO on which the number of shares of outstanding Class B common stock (including shares of Class B common stock subject to outstanding stock options) held by Tomer Weingarten, including certain permitted entities that Mr. Weingarten controls, is less than 25 % of the number of shares of outstanding Class B common stock (including shares of Class B common stock subject to outstanding stock options) that Mr. Weingarten originally held as of the date of our Final Prospectus, (iv) the date fixed by our board of directors, following the first date following the completion of our IPO when Mr. Weingarten is no longer providing services to us as an officer, employee, consultant or member of our board of directors, (v) the date fixed by our board of directors following the date on which, if applicable, Mr. Weingarten is terminated for cause, as defined in our restated certificate of incorporation, and (vi) the date that is 12 months after the death or disability, as defined in our restated certificate of incorporation, of Mr. Weingarten. This concentrated control will limit or preclude your ability to influence corporate matters for the foreseeable future, including the election of directors, amendments of our organizational documents, and any merger, consolidation, sale of all or substantially all of our assets, or other major corporate transaction requiring stockholder approval. In addition, this may prevent or discourage unsolicited acquisition proposals or offers for our capital stock that you may feel are in your best interest as one of our stockholders. Future transfers by holders of our Class B common stock will generally result in those shares converting to Class A common stock, subject to limited exceptions, such as certain transfers effected for estate planning purposes. The conversion of Class B common stock to Class A common stock will have the effect, over time, of increasing the relative voting power of those holders of our Class B common stock who retain their shares in the long term. The dual class structure of our common stock may adversely affect the trading market for our Class A common stock. We cannot predict whether our dual class structure will, over time, result in a lower or more volatile market price of our Class A common stock, adverse publicity, or other adverse consequences. Certain stock index providers ~~, such as S & P Dow Jones,~~ exclude ~~companies with~~ **or limit the ability of** multi-

class share structures from being added to certain ~~of its~~ indices ~~, including the S & P 500~~. In addition, several stockholder advisory firms and large institutional investors oppose the use of multiple class structures. As a result, the dual class structure of our common stock may make us ineligible for inclusion in certain indices ~~and~~ **,** may discourage such indices from selecting us for inclusion ~~,~~ **(** notwithstanding our automatic termination provision ~~,~~ **)** may cause stockholder advisory firms to publish negative commentary about our corporate governance practices or otherwise seek to cause us to change our capital structure, and may result in large institutional investors not purchasing shares of our Class A common stock. Any exclusion from certain stock indices could result in less demand for our Class A common stock. Any actions or publications by stockholder advisory firms or institutional investors critical of our corporate governance practices or capital structure could also adversely affect the value of our Class A common stock. **General Risk Factors** Our business depends on the overall demand..... and uncertainty in the capital markets. We may be adversely affected by natural disasters, pandemics **,** and other catastrophic events, and by man-made problems such as war **and regional geopolitical conflicts around the world** , that could disrupt our business operations, and our business continuity and disaster recovery plans may not adequately protect us from a serious disaster. Natural disasters or other catastrophic events may cause damage or disruption to our operations, international commerce, and the global economy, and thus could have an adverse effect on us. Our business operations are also subject to interruption by fire, power shortages, flooding, and other events beyond our control. In addition, our global operations expose us to risks associated with public health crises, such as pandemics and epidemics, which could harm our business and cause our operating results to suffer. ~~For example, the ongoing effects of the COVID- 19 pandemic and the measures that we, our customers and governmental authorities have adopted, as described in detail elsewhere in these risk factors, have and could continue to have an adverse effect on our business and operating results. In addition, our growth rate may actually slow or decline as the impact of the COVID- 19 pandemic tapers as people continue to return to offices and other workplaces.~~ Further, acts of war, armed conflict, terrorism and other geopolitical unrest, such as ~~Russia' s invasion of~~ **the conflicts in the Middle East,** Ukraine **and tensions between China and Taiwan** , could cause disruptions in our business or the businesses of our partners or the economy as a whole **. We maintain an office in Tel Aviv, Israel and had approximately 13 % of our personnel in Israel as of January 31, 2024. We are closely monitoring the unfolding events of the armed conflict in Israel which began in October 2023. While this conflict is still evolving, to date, the conflict has not had an adverse impact on our business results of operations and we have implemented continuity measures to address the safety of our employees and continue our operations in the event of reduced employee availability in the conflict region. However, if our continuity measures fail or the conflict continues to worsen or intensify, any business interruptions or spillover effects could adversely affect our business and operations** . In the event of a natural disaster, including a major earthquake, blizzard, or hurricane, or a catastrophic event such as a fire, power loss, cyberattack, or telecommunications failure, we may be unable to continue our operations and may endure system interruptions, reputational harm, delays in development of our platform, lengthy interruptions in service, breaches of data security, and loss of critical data, all of which could have an adverse effect on our future operating results. Climate change could result in an increase in the frequency or severity of such natural disasters. **Moreover, any of our office locations may be vulnerable to the adverse effects of climate change.** For example, our corporate offices are located in California, a state that frequently experiences earthquakes, wildfires **and resultant air quality impacts and power shutoffs associated with wildfire prevention** , heatwaves **,** and droughts **. These events can, in turn, have impacts on inflation risk, food security, water security and on our employees' health and well- being** . Additionally, all the aforementioned risks will be further increased if we do not implement an effective disaster recovery plan or our partners' disaster recovery plans prove to be inadequate. ~~The COVID- 19 pandemic could adversely affect our business, operating results, and financial condition. The COVID- 19 pandemic continues to impact worldwide economic activity and financial markets. We have experienced, and may continue to experience negative impacts on certain parts of our business. The full extent to which the COVID- 19 pandemic will directly or indirectly impact our business, operating results, cash flows, and financial condition will depend on future developments that are uncertain and cannot be accurately predicted. Measures we have taken to mitigate the spread of the virus could negatively affect our customer success efforts, delay and lengthen our sales cycle for some prospective customers and delay the delivery of professional services and trainings to our customers, impact our marketing, sales and support efforts, reduce employee efficiency and productivity, increase employee attrition, and create operational or other challenges, any of which could harm our business and results of operations. We do not yet know the full extent of potential impacts on our business, operations or on the global economy as a whole, particularly if the COVID- 19 pandemic persists for an extended period of time. Potential impacts include but are not limited to: • our customer prospects and our existing customers may experience slowdowns in their businesses, which in turn may result in reduced demand for our platform, lengthening of sales cycles, loss of customers, and difficulties in collections; • we have opened our offices in accordance with local ordinances, however, most of our employees continue to work from home and a substantial number may continue to do so for the foreseeable future, which may present challenges to employee collaboration, productivity and retention; • we continue to incur fixed costs, particularly for real estate, and are deriving reduced or no benefit from those costs; • we may continue to experience disruptions to our growth planning, such as for facilities and international expansion; • we anticipate incurring costs in returning to work from our facilities around the world, including changes to the workplace, such as space planning, food service, and amenities; • we may be subject to legal liability for safe workplace claims; and • our critical vendors could go out of business; Any of the foregoing could adversely affect our business, financial condition, and operating results.~~ Investors' expectations of our performance relating to environmental, social and governance factors may impose additional costs and expose us to new risks. There is an increasing focus from certain **regulators,** investors, employees, users and other stakeholders concerning corporate responsibility, specifically related to **ESG** ~~environmental, social and governance~~ matters ~~(ESG)~~ **both in the US and internationally** . Some investors may use these non- financial performance factors to guide their investment strategies and, in some cases, may choose not to invest in us if they believe our policies and actions relating to corporate responsibility are inadequate. We may face

reputational damage in the event that we do not meet the ESG standards set by various constituencies. ~~Furthermore ----~~ **Further** , ~~if~~ **ESG initiatives, goals or commitments could be difficult to achieve or costly to implement. If** our competitors' corporate social responsibility performance is perceived to be better than ours, potential or current investors may elect to invest with our competitors instead. **Moreover** ~~In addition~~ , **California recently adopted two new climate- related bills, which require companies doing business** in **California** ~~the event~~ that **meet** ~~we communicate~~ certain ~~initiatives and~~ **revenue thresholds to publicly disclose certain greenhouse** ~~goals~~ --- **gas emissions data** ~~regarding environmental, social~~ and ~~governance matters~~ **climate- related financial risk reports** , ~~we~~ **and compliance with such requirements** could ~~fail~~ **require significant effort and resources. Additionally** , **in March 2024, the SEC enacted comprehensive climate change disclosure rules, which have since been challenged by various third parties. Our business may face increased scrutiny related to these activities and** ~~or~~ **our related disclosures** ~~be perceived to fail~~ , ~~in our achievement of such initiatives~~ **including from the investment community, and** ~~or~~ **our** ~~goals,~~ **failure to achieve progress** or ~~we~~ **manage the dynamic public sentiment and legal landscape in these areas on a timely basis, or at all,** could **adversely affect** ~~be criticized for the scope of such initiatives or goals. If we fail to satisfy the expectations of investors, employees and other stakeholders or our initiatives are not executed as planned,~~ our reputation ~~and~~ **,** business, ~~operating results~~ and financial **performance** ~~condition could be adversely affected~~ . If industry or financial analysts do not publish research or reports about our business, or if they issue inaccurate or unfavorable research regarding our Class A common stock, our stock price and trading volume could decline. The trading market for our Class A common stock may be influenced by the research and reports that industry or financial analysts publish about us, our business, our market and our competitors. We do not control these analysts or the content and opinions included in their reports. If any of the analysts who cover us issues an inaccurate or unfavorable opinion regarding our stock price, our stock price would likely decline. If our financial results fail to meet, or significantly exceed, our announced guidance or the expectations of analysts or public investors, analysts could downgrade our Class A common stock or publish unfavorable research about us. If one or more of these analysts cease coverage of our Class A common stock or fail to publish reports on us regularly, our visibility in the financial markets could decrease, which in turn could cause our stock price or trading volume to decline. We ~~could~~ **are currently subject to and can in the future** be subject to securities class action litigation. ~~In the past, securities~~ **Securities** class action litigation **can be** ~~has often been~~ instituted against companies following periods of volatility in the market price of a company' s securities. **We are currently subject to securities litigation as further described in the section titled " Legal Proceedings. "** This type of litigation **can** ~~, if instituted, could~~ result in substantial costs and a diversion of management' s attention and resources, which could adversely affect our business, operating results, or financial condition. Additionally, the dramatic increase in the cost of directors' and officers' liability insurance may make it more expensive for us to obtain directors' and officers' liability insurance in the future and may require us to opt for lower overall policy limits and coverage or to forgo insurance that we may otherwise rely on to cover significant defense costs, settlements, and damages awarded to plaintiffs, or incur substantially higher costs to maintain the same or similar coverage. These factors could make it more difficult for us to attract and retain qualified executive officers and members of our board of directors. We do not intend to pay dividends in the foreseeable future. As a result, your ability to achieve a return on your investment will depend on appreciation in the price of our Class A common stock. We have never declared or paid any cash dividends on our capital stock. We currently intend to retain all available funds and any future earnings for use in the operation of our business and do not anticipate paying any dividends in the foreseeable future. Any determination to pay dividends in the future will be at the discretion of our board of directors. Accordingly, investors must rely on sales of their Class A common stock after price appreciation, which may never occur, as the only way to realize any future gains on their investments. Provisions in our charter documents and under Delaware law could make an acquisition of us, which may be beneficial to our stockholders, more difficult and may limit attempts by our stockholders to replace or remove our current management. Provisions in our restated certificate of incorporation and amended and restated bylaws may have the effect of delaying or preventing a merger, acquisition or other change of control of the company that the stockholders may consider favorable. In addition, because our board of directors is responsible for appointing the members of our management team, these provisions may frustrate or prevent any attempts by our stockholders to replace or remove our current management by making it more difficult for stockholders to replace members of our board of directors. Among other things, our restated certificate of incorporation and amended and restated bylaws include provisions that: • provide that our board of directors is classified into three classes of directors with staggered three- year terms; • permit our board of directors to establish the number of directors and fill any vacancies and newly created directorships; • require super- majority voting to amend some provisions in our restated certificate of incorporation and amended and restated bylaws; • authorize the issuance of " blank check " preferred stock that our board of directors could use to implement a stockholder rights plan; • provide that only our chief executive officer or a majority of our board of directors will be authorized to call a special meeting of stockholders; • eliminate the ability of our stockholders to call special meetings of stockholders; • do not provide for cumulative voting; • provide that directors may only be removed " for cause " and only with the approval of two- thirds of our stockholders; • provide for a dual class common stock structure in which holders of our Class B common stock may have the ability to control the outcome of matters requiring stockholder approval, even if they own significantly less than a majority of the outstanding shares of our common stock, including the election of directors and other significant corporate transactions, such as a merger or other sale of our company or its assets; • prohibit stockholder action by written consent, which requires all stockholder actions to be taken at a meeting of our stockholders; • provide that our board of directors is expressly authorized to make, alter, or repeal our amended and restated bylaws; and • establish advance notice requirements for nominations for election to our board of directors or for proposing matters that can be acted upon by stockholders at annual stockholder meetings. Moreover, Section 203 of the Delaware General Corporation Law (DGCL), may discourage, delay, or prevent a change in control of our company. Section 203 imposes certain restrictions on mergers, business combinations, and other transactions between us and holders of 15 % or more of our common stock. Our restated certificate of incorporation contains exclusive forum provisions for certain claims,

which may limit our stockholders' ability to obtain a favorable judicial forum for disputes with us or our directors, officers, or employees. Our restated certificate of incorporation provides that the Court of Chancery of the State of Delaware, to the fullest extent permitted by law, will be the exclusive forum for any derivative action or proceeding brought on our behalf, any action asserting a breach of fiduciary duty, any action asserting a claim against us arising pursuant to the DGCL, our restated certificate of incorporation, or our amended and restated bylaws, or any action asserting a claim against us that is governed by the internal affairs doctrine. Moreover, Section 22 of the Securities Act creates concurrent jurisdiction for federal and state courts over all claims brought to enforce any duty or liability created by the Securities Act or the rules and regulations thereunder. Our restated certificate of incorporation provides that the federal district courts of the **US** ~~United States~~ will, to the fullest extent permitted by law, be the exclusive forum for resolving any complaint asserting a cause of action arising under the Securities Act **(** ~~, or~~ Federal Forum Provision **)**. Our decision to adopt a Federal Forum Provision followed a decision by the Supreme Court of the State of Delaware holding that such provisions are facially valid under Delaware law. While there can be no assurance that federal or state courts will follow the holding of the Delaware Supreme Court or determine that the Federal Forum Provision should be enforced in a particular case, application of the Federal Forum Provision means that suits brought by our stockholders to enforce any duty or liability created by the Securities Act must be brought in federal court and cannot be brought in state court. Section 27 of the Exchange Act creates exclusive federal jurisdiction over all claims brought to enforce any duty or liability created by the Exchange Act or the rules and regulations thereunder. In addition, the Federal Forum Provision applies to suits brought to enforce any duty or liability created by the Exchange Act. Accordingly, actions by our stockholders to enforce any duty or liability created by the Exchange Act or the rules and regulations thereunder must be brought in federal court. Our stockholders will not be deemed to have waived our compliance with the federal securities laws and the regulations promulgated thereunder. Any person or entity purchasing or otherwise acquiring or holding any interest in any of our securities shall be deemed to have notice of and consented to our exclusive forum provisions, including the Federal Forum Provision. These provisions may limit a stockholders' ability to bring a claim in a judicial forum of their choosing for disputes with us or our directors, officers, or employees, which may discourage lawsuits against us and our directors, officers, and employees. Alternatively, if a court were to find the choice of forum provision contained in our restated certificate of incorporation or amended and restated bylaws to be inapplicable or unenforceable in an action, we may incur additional costs associated with resolving such action in other jurisdictions, which could harm our business, financial condition, and operating results. ~~62~~