**Risk Factors Comparison 2025-02-28 to 2024-03-04 Form: 10-K**

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

Investing in our securities 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 related notes, before making a decision to invest in our securities. The risks and uncertainties described below may not be the only ones we face. If any of the risks actually occur, our business could be materially and adversely affected. In that event, the market price of our Class A common stock could decline, and you could lose part or all of your investment. Risks Related to Our Business and Our Industry Our business depends on our ability to attract new customers, retain and upsell additional products and new product categories to existing customers, and upgrade free users to our paid offerings. Any decline in new customers, renewals, or upgrades would harm our business. Our business depends upon our ability to attract new customers, and maintain and expand our relationships with our existing customers, including upselling additional products and new product categories to our existing customers and upgrading users from a free plan to one of our paid offerings. Our business is subscription based, and customers are not obligated to, and may choose not to, renew their subscriptions after their existing subscriptions expire. Customers may also terminate or reduce the size of their existing subscriptions. As a result, we cannot provide assurance that customers will renew their subscriptions utilizing the same tier of plan, upgrade to a higher- priced tier, or purchase additional products, if they renew at all. Renewals of subscriptions to our platform may decline or fluctuate because of several factors, such as dissatisfaction with our products and support, a customer no longer having a need for our products, or a belief that a competitor' s product is better, more secure, or less expensive than our products and platform. For example, during the COVID- 19 pandemic, we saw a significant increase in usage and subscriptions. As a result, our customer base shifted largely from businesses and enterprises to a mix of businesses, enterprises, and consumers. Following the pandemic, some of our customers reduced or discontinued their use of our platform, and additional customers may do so in the future. Additionally, this shift in mix has resulted and may continue to result in higher non- renewal rates than we have experienced in the past. Renewals are also impacted by reductions in customer information technology spending budgets or a decision by the customer to consolidate their spending budgets on one of our competitor' s platforms, both of which are more likely to occur during periods of high inflation or recessionary or uncertain economic environments. We must continually add new customers and licenses to grow our business and to replace customers and licenses who choose not to continue to use our platform. Finally, any decrease in user satisfaction with our products or support would harm our brand, word- of- mouth referrals, and ability to grow. We encourage customers to purchase additional products and encourage users of our free offering to upgrade to one of our paid offerings by recommending additional features and through in- product prompts and notifications. However, free users may never upgrade to one of our paid offerings. We also seek to expand within organizations by adding new licenses, having workplaces purchase additional products, or expanding the use of our platform into other teams and departments within an organization. If we fail to upsell our customers or upgrade free users to one of our paid offerings or expand the number of licenses within organizations, our business would be harmed. Our revenue growth rate has fluctuated in prior periods, and may continue to decline in future periods. Our revenue growth has fluctuated in prior periods. You should not rely on the revenue growth of any prior quarterly or annual period as an indication of our future performance. There are no assurances we will be able to sustain ~~or increase~~ our revenue growth in future periods, and our revenue growth rate may continue to **remain flat or** decline in future periods. Many factors **have and** may contribute to declines in our growth rate, including higher market penetration, increased competition, macroeconomic conditions, such as inflation, recessionary or uncertain economic environments, fluctuating foreign currency exchange rates, slowing demand for our platform, a lower than anticipated capitalization on growth opportunities, and the maturation of our business, among others. Our growth rate could adversely affect investors' perceptions of our business and the trading price of our Class A common stock could be adversely affected. Interruptions, delays, or outages in service from our co- located data centers **or cloud hosting services** and a variety of other factors, would impair the delivery of our services, require us to issue credits or pay penalties, and harm our business. We currently serve our users from various co- located data centers located throughout the world. We also utilize **cloud hosting services such as** Amazon Web Services and Oracle Cloud for the hosting of certain critical aspects of our business **and** ~~, as well as~~ Microsoft Azure for limited customer- specified managed services. As part of our distributed meeting architecture, we establish private links between data centers that automatically transfer data between various data centers. Damage to, or failure of, these data centers has in the past resulted in and could in the future result in interruptions or delays in our services. In addition, we have experienced, and may in the future experience, other interruptions and delays in our services caused by a variety of other factors, including, but not limited to, infrastructure changes, vendor **(including cloud hosting)** issues, human or software errors, viruses, security attacks, ransomware or cyber extortion, fraud, general internet availability issues, spikes in usage, local administrative actions, changes to legal or permitting requirements, and denial of service issues. In some instances, we may not be able to identify the cause or causes of these problems within an acceptable period of time. For example, we have experienced partial outages in our services that impacted a subset of our users for a limited number of hours. Additionally, in connection with the addition of new data centers or expansion or consolidation of our existing data center facilities or other reasons, we may move or transfer our data and our users' metadata to other data centers, not including our China data center. Despite precautions that we take during this process, any unsuccessful data transfers may impair or cause disruptions in the delivery of our service, and we may incur significant costs in connection with any such move or transfer. Interruptions, delays,

or outages in our services would reduce our revenue; may require us to issue credits or pay penalties; may subject us to claims and litigation; and may cause customers to terminate their subscriptions and adversely affect our ability to attract new customers. Our ability to attract and retain customers and licenses depends on our ability to provide customers and users with a highly reliable platform and even minor interruptions or delays in our services could harm our business. Additionally, if our data centers **or cloud hosting services** are unable to keep up with our increasing needs for capacity, customers may experience delays or interruptions in service as we seek to obtain additional capacity, which could result in the loss of customers who use our unified communications and collaboration platform because of its reliability and performance. We plan to continue our practice of opening new co- located data centers throughout the world to meet increased demand, but we may be unable to bring additional data centers online in a timely manner, including as a result of current shortages for certain parts, such as servers. We do not control, or in some cases have limited control over, the operation of the co- located data center facilities **and cloud hosting services** we use, and they are vulnerable to damage or interruption from human error; intentional bad acts; earthquakes; floods; fires; hurricanes; war; terrorist attacks; power losses; hardware failures; systems failures; telecommunications failures; disease; and other public health related measures, any of which could disrupt our service. In the event of significant physical damage to one of these data centers **or disruption of the cloud hosting services we use** , it may take a significant period of time to achieve full resumption of our services and our disaster recovery planning may not account for all eventualities. Despite precautions taken at these **data center** facilities, the occurrence of a natural disaster, an act of terrorism, or other act of malfeasance, a decision to close the facilities without adequate notice or other unanticipated problems at the facilities would harm our business. We operate in competitive markets, and we must continue to compete effectively. The market for communication and collaboration technologies platforms is competitive and rapidly changing ~~,~~ and ~~existing and~~ **includes companies ranging from** new market entrants **to hyperscalers** ~~, particularly established companies with greater resources than we have,~~ that provide technologies to improve communication and collaboration technologies platforms **either** ~~, such~~ as ~~AI~~ **bundled solutions or standalone products. Given the range of companies in this space, maintaining** ~~and~~ **an open and robust marketplace with fair** ~~machine learning, could also increase the level of~~ competition **is important** ~~in the market~~ . Certain features of our current platform compete in the communication and collaboration technologies market with products offered by: • bundled productivity ~~solutions~~ **suite** providers with ~~video functionality~~ **communication offerings** , including Microsoft **365 (with** Teams **)** and Google ~~G Suite and~~ **Workspace (with** Meet ~~products~~ **)** ; • legacy web- based meeting providers, including Cisco Webex and GoTo; • UCaaS and legacy PBX providers, including Avaya, RingCentral, and 8x8; and • consumer- facing platforms that can support small- or medium- sized businesses, including Amazon, Apple, and Facebook. Other large established companies may also make investments in video communications tools. In addition, as we introduce new products and services into our platform, and with the introduction of new technologies and market entrants, including AI, we expect competition to **continue to** intensify ~~in the future~~ . In February 2022, we launched Zoom Contact Center, an omnichannel contact center solution that is optimized for video, which competes against companies that offer similar services, such as Five9, ~~Inc.,~~ Genesys **,** and NICE inContact, and new competitors that may enter that market in the future. As we continue to build out our platform, we may face increased competition against companies that offer similar services and new competitors that may enter that market in the future. During the COVID- 19 pandemic, we saw a significant increase in usage and subscriptions from smaller customers, many of whom are consumers or small and medium sized businesses. With respect to these smaller customers, we face competition from more consumer- oriented platforms, most of which have more experience with the consumer market than we do. Further, many of our actual and potential competitors benefit from competitive advantages over us, such as greater name recognition; longer operating histories; more varied products and services; larger marketing budgets; more established marketing **, customers and partner** relationships; more third- party ~~integration~~ **integrations** ; greater accessibility across devices ~~or~~ **and** applications; greater access to larger user bases; major distribution agreements with hardware manufacturers and resellers; and greater financial, technical, and other resources. Some of our competitors may make acquisitions or strategic investments or enter into strategic relationships to offer a broader range of products and services than we do, which may prevent us from using such third parties' technology or offering such products or services. These combinations may make it more difficult for us to compete effectively. We expect these trends to continue as competitors attempt to strengthen or maintain their market positions. Demand for our platform is also price sensitive. Many factors, including our marketing, user acquisition, and technology costs, and our current and future competitors' pricing and marketing strategies, can significantly affect our pricing strategies. Certain competitors offer, or may in the future offer, lower-priced or free products, or services that compete with our platform, or may bundle and offer a broader range of products and services than we do. Similarly, certain competitors may use marketing strategies that enable them to acquire customers at a lower cost than we can. Furthermore, third parties could build products similar to ours that rely on open source software. Even if such products do not include all the features and functionality that our platform provides, we could face pricing pressure from these third parties to the extent that users find such alternative products to be sufficient to meet their needs. **In some cases,** ~~There can be no assurance that~~ we **have been** ~~will not be~~ forced to engage in price- cutting initiatives or other discounts ~~or to increase our marketing and other expenses~~ to attract and retain customers in response to competitive pressures, ~~either of which would harm our business~~ **and may have to do so in the future** . We, on occasion, offer customers a free period of time at the beginning of the subscription term that can result in deferred billings or long- term accounts receivable and increase the risk of loss on uncollected accounts receivable. Our results have fluctuated and may in the future fluctuate significantly and may not fully reflect the underlying performance of our business. Our results of operations have fluctuated and may in the future fluctuate significantly, and period- to- period comparisons of our results of operations may not be meaningful. Accordingly, the results of any one quarter should not be relied upon as an indication of future performance. Our results of operations may fluctuate as a result of a variety of factors, many of which are outside of our control, and as a result, may not fully reflect the underlying performance of our business. For example, during fiscal year 2021, we experienced rapid growth in usage of our

unified communications and collaboration platform largely due to the COVID- 19 pandemic, a significant portion of which was attributable to free Basic accounts, which do not generate any revenue. To meet this increased demand, we have incurred and expect to continue to incur significant costs associated with upgrading our infrastructure and expanding our capacity. ~~Fluctuation~~ **Fluctuations** in our results may negatively impact the value of our securities. Factors that may cause fluctuations in our results of operations include, without limitation, those listed below: • our ability to retain and upgrade customers to higher- priced plans; • our ability to attract new customers and upgrade free users to one of our paid offerings; • our ability to hire and retain employees, in particular those responsible for the selling or marketing of our platform; • our ability to hire, develop, and retain talented sales personnel who are able to achieve desired productivity levels in a reasonable period of time and provide sales leadership in areas in which we are expanding our sales and marketing efforts; • changes in the way we organize and compensate our sales teams; • the timing of expenses and recognition of revenue; • our ability to increase sales to large organizations; • the length of our sales cycles and linearity of our bookings, especially with respect to sales to large enterprises and highly regulated industries, including financial services and U. S. federal and state and foreign governmental agencies; • the amount and timing of operating expenses related to the maintenance and expansion of our business, operations, and infrastructure, as well as international expansion and entry into operating leases, and the hiring and retention of personnel who can build, manage, and maintain our expanded business operations and infrastructure; • timing and effectiveness of new sales and marketing initiatives; • changes in our pricing policies or those of our competitors; • our ability to hire and retain experienced research and development personnel to design new products, features, and functionality that meet our privacy and security standards; • the timing and success of new products, features, and functionality by us or our competitors; • interruptions or delays in our service, network outages, or actual, alleged, or perceived privacy violations or issues or security vulnerabilities, incidents, or breaches; • lawsuits, regulatory actions or investigations, legislator scrutiny, or negative publicity arising from actual, alleged, or perceived privacy violations or issues or security vulnerabilities, incidents, or breaches; • changes in the competitive dynamics of our industry, including consolidation among competitors; • changes in laws and regulations that impact our business; • any large indemnification payments to our users or other third parties; • the timing of expenses related to any future acquisitions; and • general economic and market conditions. Our business may be significantly affected by changes in the economy, including any resulting effect on consumer or business spending. Our business may be significantly affected by changes in the economy, such as high inflation and the responses by central banking authorities to control such inflation, recessionary or uncertain environments, ~~U. S. federal debt ceiling negotiations and the risk of a U. S. government shutdown,~~ fluctuations in the foreign currency exchange rates and ~~global impacts~~ **geopolitical tensions and military conflicts** , including the **ongoing conflicts between** ~~Russian~~ **Russia and** ~~invasion of~~ Ukraine ~~, the conflict in Israel~~ and **in** the ~~surrounding area~~ **Middle East,** and **tariffs and trade tensions, including** the United States' ongoing trade disputes with China and other countries. While some customers may view a subscription to our platform as a cost- saving purchase, decreasing the need for business travel, others may view a subscription to our platform as a discretionary purchase, and our customers may reduce their information technology spending on our platform during an economic downturn or during times of economic uncertainty. Given current economic conditions, including inflation, we have experienced and may continue to experience a loss of users and customers, as well as a reduction in demand for our platform, especially if the effects of the current economic environment have a prolonged impact on various industries that our unified communications and collaboration platform addresses. In addition to the foregoing, adverse developments that affect financial institutions, transactional counterparties or other third parties, such as bank failures, or concerns or speculation about any similar events or risks, could lead to market- wide liquidity problems, which in turn may cause third parties, including customers, to become unable to meet their obligations under various types of financial arrangements as well as general disruptions or instability in the financial markets. Moreover, we have lost and may continue to lose customers as a result of such customers ceasing to do business, and we have experienced and may continue to experience a material increase in longer payment cycles and greater difficulty in collecting accounts receivable from certain customers. These issues may continue in the future if current economic conditions continue or worsen. As we increase sales to large organizations, our sales cycles have and could continue to lengthen, and we could experience greater deployment challenges. We invest significant resources into sales to large organizations. Large organizations typically undertake a significant evaluation and negotiation process due to their leverage, size, organizational structure, and approval requirements, all of which have and may continue to lengthen our sales cycle. We have also faced and may in the future face unexpected deployment challenges with large organizations or more complicated deployment of ~~our~~ some or all aspects of our platform. Large organizations may demand additional features, support services and pricing concessions, or require additional security management or control features. We may spend substantial time, effort, and money on sales efforts to large organizations without any assurance that our efforts will produce any sales or that these customers will deploy our platform widely enough across their organization to justify our substantial up- front investment. As a result, we anticipate increased sales to large organizations will lead to higher up- front sales costs and greater unpredictability in our business, results of operations, and financial condition. We generate revenue from sales of subscriptions to our platform, and any decline in demand for our platform or for communications and collaboration technologies in general would harm our business. We generate, and expect to continue to generate, revenue from the sale of subscriptions to our platform. As a result, widespread acceptance and use of communications and collaboration technologies in general, and our platform in particular, is critical to our future growth and success. If the communications and collaboration technologies market fails to grow, or grows more slowly than we currently anticipate, demand for our platform could be negatively affected. Changes in user preferences for communications and collaboration technologies may have a disproportionately greater impact on us than if we offered multiple platforms or disparate products. Demand for communications and collaboration technologies in general, and our platform in particular, is affected by a number of factors, many of which are beyond our control. Some of these potential factors include: • general awareness of the communications and collaboration technologies category; • availability of products and services that compete with ours; • new modes of

communications and collaboration that may be developed in the future; • a reduction in customer information technology spending budgets, or a consolidation of spending budgets on our competitors' platforms, especially during periods of inflation or recessionary or uncertain economic environments; • ease of adoption and use; • features and platform experience; • reliability of our platform, including frequency of outages; • performance; • brand; • user support; and • pricing. The communications and collaboration technologies market is subject to rapidly changing user demand and trends in preferences. If we fail to successfully predict and address these changes and trends, meet user demands, or achieve more widespread market acceptance of our platform, our business would be harmed. We have incurred net losses in the past and there are no assurances we will be able to maintain or increase profitability in the future. We have incurred net losses in the past and could incur net losses in the future. We intend to continue to expend significant funds on our sales and marketing efforts to attract new customers, expand the number of licenses and services used by our customers and develop and enhance our products. We also intend to continue investing in general corporate purposes, including operations, hiring additional personnel, including through acquisitions of other businesses, upgrading our infrastructure, addressing security and privacy issues, and expanding into new geographies and markets. To the extent we are successful in increasing our customer base, we may also incur increased losses because, other than sales commissions, the costs associated with acquiring customers are generally incurred up front, while the subscription revenue is generally recognized ratably over the subscription term, which can be monthly, annual, or on a multiyear basis. Our efforts to grow our business may be costlier than we expect, and we may not be able to increase our revenue enough to offset our higher operating expenses, which may result in decreased profitability. We may incur significant losses in the future for a number of reasons, including as a result of the other risks described herein, and unforeseen expenses, difficulties, complications, delays, and other unknown events. While free users continue to be a meaningful portion of the user base, we have directed marketing programs focused on converting free users to paid subscriptions. Some of these users have upgraded to a paid plan but the remainder have not and may never do so. If we are unable to increase or sustain our profitability, the value of our business and Class A common stock may significantly decrease. Furthermore, it is difficult to predict the size and growth rate of our market, customer demand for our platform, customer adoption and renewal of our platform, the entry of competitive products and services, or the success of existing competitive products and services. As a result, we may not **be able to** increase or maintain profitability in future periods. If we fail to grow our revenue sufficiently to keep pace with our investments and other expenses, our business would be harmed. The experience of our users depends upon the interoperability of our platform across devices, operating systems, and third- party applications that we do not control, and if we are not able to maintain and expand our relationships with third parties to integrate our platform with their solutions, our business may be harmed. One of the most important features of our platform is its broad interoperability with a range of diverse devices, operating systems, and third-party applications. Our platform is accessible from the web and from devices running Windows, Mac OS, iOS, Android, and Linux. We also have integrations with Atlassian, Dropbox, Google, Microsoft, Salesforce, Slack, and a variety of other productivity, collaboration, data management, and security vendors. We are dependent on the accessibility of our platform across these and other third- party operating systems and applications that we do not control, and some of these third parties can make it more difficult for our platform to interoperate with their systems in favor of competitive platforms. For example, given the broad adoption of Microsoft Office and other productivity software, it is important that we are able to integrate with this software. Several of our competitors own, develop, operate, or distribute operating systems, app stores, co- located data center services, and other software, and also have material business relationships with companies that own, develop, operate, or distribute operating systems, applications markets, co- located data center services, and other software that our platform requires in order to operate. Moreover, some of these competitors have inherent advantages developing products and services that more tightly integrate with their software and hardware platforms or those of their business partners. Third- party services and products are constantly evolving, and we may not be able to modify our platform to assure its compatibility with that of other third parties following development changes. In addition, some of our competitors may be able to disrupt the operations or compatibility of our platform with their products or services, or exert strong business influence on our ability to, and terms on which we, operate and distribute our platform. For example, we currently offer products that directly compete with several large technology companies that we rely on to ensure the interoperability of our platform with their products or services. As our respective products evolve, we expect this level of competition to increase. Should any of our competitors modify their products or standards in a manner that degrades the functionality of our platform or gives preferential treatment to competitive products or services, whether to enhance their competitive position or for any other reason, the interoperability of our platform with these products could decrease and our business could be harmed. In addition, we provide, develop, and create applications for our platform partners that integrate our platform with our partners' various offerings. For example, our Zoom ~~One~~ **Workplace** product integrates with tools offered by companies, such as Atlassian and Dropbox, to help teams get more done together. If we are not able to continue and expand on existing and new relationships to integrate our platform with our partners' solutions, or there are quality issues with our products or service interruptions of our products that integrate with our partners' solutions, our business will be harmed. We are subject to requirements imposed by app stores such as those operated by Apple and Google, who may change their technical requirements or policies in a manner that adversely impacts the way in which we or our partners collect, use and share data from users. For example, Apple recently began requiring mobile applications using its iOS mobile operating system to obtain a user' s permission to track them or access their device' s advertising identifier for certain purposes. The long- term impact of these and any other privacy and regulatory changes remains uncertain. If we do not comply with applicable requirements imposed by app stores, we could lose access to the app store and users, and our business would be harmed. We may not be able to respond to rapid technological changes, extend our platform, or develop new features. The communications and collaboration technologies market is characterized by rapid technological change and frequent new product and service introductions. Our ability to grow our customer base and increase our revenue will depend heavily on our ability to enhance and improve our platform; introduce new features and products; and interoperate across an increasing range of devices,

operating systems, and third- party applications. Our customers may require features and capabilities that our current platform does not have. In particular, advancements in technology such as AI and machine learning are changing the way people work, and businesses that are slow to adopt these new technologies may face a competitive disadvantage. We invest significantly in research and development, and our goal is to focus our spending on measures that improve quality and ease of adoption, enhance privacy and security, and create organic demand for our platform. There is no assurance that new additions or other future enhancements to our platform or new product experiences, features, or capabilities will be compelling to our customers or gain market acceptance, or that they will perform as expected. If our research and development investments do not accurately anticipate demand or if we fail to develop our platform in a manner that satisfies customer preferences and requirements in a timely and cost- effective manner, we may fail to retain our existing customers or increase demand for our platform. The introduction of new products and services by competitors or the development of entirely new technologies to replace existing offerings, such as AI- powered communication and collaboration tools, could make our platform obsolete or adversely affect our business, results of operations, and financial condition. We may experience difficulties with software development, design, or marketing that could delay or prevent our development, introduction, or implementation of new product experiences, features, or capabilities. We have in the past experienced delays in our internally planned release dates of new features and capabilities and there can be no assurance that new product experiences, features, or capabilities will be released according to schedule. Any delays could result in adverse publicity, loss of revenue or market acceptance, or claims by users brought against us, all of which could harm our business. Moreover, new productivity features to our platform may require substantial investment, and we have no assurance that such investments will be successful. If customers and users do not widely adopt our new product experiences, features, and capabilities, or they do not perform as expected, we may not be able to realize a return on our investment. If we are unable to develop, license, or acquire new features and capabilities to our platform on a timely and cost- effective basis, or if such enhancements do not achieve market acceptance, our business would be harmed. We use generative AI including in our products and services, which may result in operational challenges, legal liability, reputational concerns, competitive risks and regulatory concerns that could adversely affect our business and results of operations. We use generative AI processes and algorithms, including by deploying generative AI features in our products and services, which may result in adverse effects to our operations, legal liability, reputation and competitive risks. The use of generative **and agentic** AI at scale is relatively new, and may lead to challenges, concerns and risks that are significant or that we may not be able to predict. For example, AI algorithms use machine learning (" ML ") and predictive analytics which may be insufficient, biased, inaccurate or of poor quality, which could result in customer rejection or skepticism of our products, adversely impact the rights of individuals, affect our reputation or brand, and negatively affect our financial results. Additionally, we **rely on third parties for certain AI features of our products and if such third parties do not provide us those features (or do not do so on acceptable terms), experience interruptions, or cease operating, we may need to work with another provider, which may take time or may not be possible, and** could **result in the disruption of certain of our products or services, affect our reputation or brand, and negatively affect our financial results. We could also** face claims from third parties claiming infringement of their intellectual property or other proprietary rights with respect to materials used or created by generative **or agentic** AI tools or features that we believed to be available for use and not subject to such rights. The investment required to bring AI features to market and the costs associated with providing these features to our customers may be significant, and we may be unable to recover these costs if customers and users do not widely adopt these features **. We currently offer our AI features at no additional cost, as we believe they will ultimately enhance user satisfaction, improve customer retention, and drive revenue. If such benefits are not realized, the associated investment costs could further negatively impact our margins** . Further, use of generative AI tools by our employees or others could result in disclosure of confidential or sensitive company and customer data, reputational harm, and legal liability. The failure to effectively develop and expand our marketing and sales capabilities could harm our ability to increase our customer base and achieve broader market acceptance of our platform. Our ability to increase our customer base and achieve broader market acceptance of our products and services will depend to a significant extent on our ability to expand our marketing and sales operations. We plan to continue expanding our sales and marketing capabilities, including through strategic partners, both domestically and internationally. If we are unable to expand our sales and marketing operations, our future revenue growth and business could be adversely impacted. Identifying and recruiting qualified sales representatives and training them is time consuming and resource intensive, and they may not be fully trained and productive for a significant amount of time. We also plan to dedicate significant resources to sales and marketing programs, including internet and other online advertising. All of these efforts will require us to invest significant financial and other resources, as the cost to acquire customers through these efforts is high. Our business will be harmed if our efforts do not generate a correspondingly significant increase in revenue. Failures in internet infrastructure or interference with broadband access could cause current or potential users to believe that our systems are unreliable, possibly leading our customers to switch to our competitors, or to cancel their subscriptions to our platform. Unlike traditional communications and ~~collaborations~~ **collaboration** technologies, our services depend on our users' high- speed broadband access to the internet, usually provided through a cable or digital subscriber line connection. Increasing numbers of users and increasing bandwidth requirements may degrade the performance of our platform due to capacity constraints and other internet infrastructure limitations. As our number of users has grown and their usage of communications capacity has increased, we have been required to make additional investments in network capacity to maintain adequate data transmission speeds, the availability of which may be limited, or the cost of which may be on terms unacceptable to us. If adequate capacity does not continue to be available to us to support our user base in the future, our network may be unable to achieve or maintain sufficiently high data transmission capacity, reliability, or performance. In addition, if internet service providers and other third parties providing internet services have outages or deteriorations in their quality of service, our users will not have access to our platform or may experience a decrease in the quality of our platform. Furthermore, as the rate of adoption of new technologies increases, the networks our platform

relies on may not be able to sufficiently adapt to the increased demand for these services, including ours. Frequent or persistent interruptions could cause current or potential users to believe that our systems or platform are unreliable, leading them to switch to our competitors or to avoid our platform, which could permanently harm our business. In addition, users who access our platform through mobile devices, such as smartphones and tablets, must have a high- speed connection, such as 3G, 4G, 5G, LTE, satellite, or Wi- Fi, to use our services and applications. Currently, this access is provided by companies that have significant and increasing market power in the broadband and internet access marketplace, including incumbent phone companies, cable companies, satellite companies, and wireless companies. Some of these providers offer products and subscriptions that directly compete with our own offerings, which can potentially give them a competitive advantage. Also, these providers could take measures that degrade, disrupt, or increase the cost of user access to third- party services, including our platform, by restricting or prohibiting the use of their infrastructure to support or facilitate third- party services or by charging increased fees to third parties or the users of third- party services, any of which would make our platform less attractive to users and reduce our revenue. On January 4, 2018, the Federal Communications Commission (" FCC ") released an order reclassifying broadband internet access as an information service, a regulatory regime generally referred to as network neutrality, subject to certain provisions of Title I of the Communications Act. The order requires broadband providers to publicly disclose accurate information regarding network management practices, performance characteristics, and commercial terms of their broadband internet access services sufficient to enable consumers to make informed choices regarding the purchase and use of such services, and entrepreneurs and other small businesses to develop, market, and maintain internet offerings. The new rules went into effect on June 11, 2018. Numerous parties filed judicial challenges to the order, and on October 1, 2019, the United States Court of Appeals for the District of Columbia Circuit released a decision that rejected nearly all of the challenges to the new rules, but reversed the FCC' s decision to prohibit all state and local regulation targeted at broadband internet service, requiring case- by- case determinations as to whether state and local regulation conflicts with the FCC' s rules. The court also required the FCC to reexamine three issues from the order but allowed the order to remain in effect, while the FCC conducts that review. On October 27, 2020, the FCC adopted an order concluding that the three issues remanded by the court did not provide a basis to alter its conclusions in the 2018 order. On October 19, 2023, the FCC adopted a notice of proposed rulemaking **proposing to reinstate the 2015 rules, and on April 24, 2024, adopted an order** that ~~would substantially reinstate~~ **reinstated** ~~the 2018 rules and asked for comment on that proposal and on potential changes to~~ those rules **. On January 2, 2025, the U. S. Court of Appeals for the Sixth Circuit issued a decision overturning the FCC order. That decision remains subject to potential further appeals** . We cannot predict ~~whether or when~~ the ~~FCC will adopt~~ **impact of the** new rules ~~or the impact of any rules that may be adopted~~ on our operations or business. In addition, a number of states have adopted or are adopting or considering legislation or executive actions that would regulate the conduct of broadband providers **, including legislation to impose state- level network requirements in New York** . After a federal court judge denied a request for a preliminary injunction against California' s state- specific network neutrality law, California began enforcing that law on March 25, 2021. A number of other states have adopted or are adopting or considering legislation or executive actions that would regulate the conduct of broadband providers. A similar law in Vermont is subject to a pending challenge, but went into effect on April 20, 2022 and the challenge has been suspended until an appeal in another case addressing state powers to adopt internet regulation is resolved. **The FCC' s April 24 order, which, as described above, was overturned by the Sixth Circuit Court of Appeals, permits it to preempt any state- level network neutrality requirements that go beyond the requirements adopted in that order, but specifically held that the California law would not be preempted.** We cannot predict whether the FCC order or other state initiatives will be enforced, modified, overturned, or vacated by legal action of the court, federal legislation, or the FCC. ~~In addition, the status of state regimes may be affected by the FCC' s action in its new network neutrality proceeding.~~ Under the FCC' s ~~current~~ **2018** rules **, which currently remain in effect** , broadband internet access providers may be able to charge web- based services such as ours for priority access or favor services offered by our competitors or by the internet access providers themselves, which could result in increased costs and a loss of existing customers, impair our ability to attract new customers, and harm our business **but the 2024 rules, if they go into effect, are intended to limit the ability of broadband internet access providers to engage in such behavior** . If there are changes to the regulatory structures in the United States or elsewhere that reduce investment in infrastructure by internet service providers, including a return of the network neutrality regulations that were ~~repealed~~ **overturned** , any impacts of reduced investment that reduce network capacity or speed could have a negative effect on our business, operating results, and financial condition. Our security measures, and those of third parties ~~upon which~~ **with whom** we ~~rely~~ **work** , have been compromised in the past and may be compromised in the future. If our security measures are compromised in the future or if our information technology fails, this could harm our reputation, expose us to significant fines and liability, impair our sales, and harm our business. In addition, **if** our products and services **are** ~~may be~~ perceived as not being secure ~~.~~ **, This this could** ~~perception may~~ result in customers and users curtailing or ceasing their use of our products, our incurring significant liabilities, and our business being harmed. In the ordinary course of our business, we and the third parties ~~upon which~~ **with whom** we ~~rely~~ **work** collect, receive, store, process, generate, use, transfer, disclose, make accessible, protect, secure, dispose of, transmit, and share confidential, proprietary, and sensitive data, including data of ours, our customers, and our users, the data which includes personal information, customer and user content, health- related data, intellectual property, trade secrets, business plans, and financial information. We and the third parties upon which we rely face a variety of evolving threats, including but not limited to ransomware attacks, which could cause security incidents. **We routinely investigate** ~~Security~~ **security** incidents **, which** have occurred in the past and may occur in the future, **that** ~~resulting~~ **result** in unauthorized access to, loss or unauthorized disclosure of, or inadvertent disclosure of confidential, proprietary, and sensitive information. Cyberattacks, other malicious internet- based activity, online and offline fraud, and other similar activities threaten the confidentiality, integrity, and availability of our proprietary, confidential, and sensitive data and information technology systems, and those of the third parties

~~upon which~~ **with whom** we ~~rely~~ **work** . Cloud- based platform providers of products and services have been and are expected to continue to be targeted. Threats are prevalent and continue to rise, are increasingly difficult to detect, and come from a variety of sources, including traditional computer " hackers, " threat actors, " hacktivists, " organized criminal threat actors, personnel (such as through theft or misuse), sophisticated nation- state and nation- state supported actors, and advanced persistent threat intrusions. Some actors now engage and are expected to continue to engage in cyberattacks, including without limitation nation-state actors for geopolitical reasons and in conjunction with military conflicts and defense activities. During times of war and other major conflicts, we and the third parties ~~upon which~~ **with whom** we ~~rely~~ **work** may be vulnerable to a heightened risk of these attacks, which could materially disrupt our systems and operations, supply chain, and ability to provide our services. We ~~may be~~ **and the third parties with whom we work are** subject to a variety of evolving threats, including but not limited to social- engineering attacks (including through deep fakes, which may be increasingly more difficult to identify as fake, and phishing attacks), malicious code (such as viruses and worms), malware (including as a result of advanced persistent threat intrusions), denial- of- service attacks, credential stuffing, personnel misconduct or error, supply- chain attacks, software bugs, server malfunctions, software or hardware failures, loss of data or other information technology assets, adware, telecommunications failures, attacks enhanced or facilitated by AI, earthquakes, fires, floods, and other similar threats. Ransomware attacks, including those perpetrated by organized criminal threat actors, nation- states, and nation- state- supported actors, are becoming increasingly prevalent and severe and can lead to significant interruptions in our operations or our ability to provide our products or services, loss of data and income, reputational harm, and diversion of funds. Extortion payments may alleviate the negative impact of a ransomware attack, but we may be unwilling or unable to make such payments due to, for example, applicable laws or regulations prohibiting such payments. Additionally, our platform, products, and services are relied on by a large number of companies worldwide and as a result, if our platform, products, or solutions are compromised, a significant number or all of our customers and their data could be simultaneously affected. The potential liability and associated consequences we could suffer as a result of such a large- scale event could be catastrophic and result in irreparable harm. Future or past business transactions (such as acquisitions or integrations) could expose us to additional cybersecurity risks and vulnerabilities, as our systems could be negatively affected by vulnerabilities present in acquired or integrated entities' systems and technologies. Furthermore, we **have discovered, and** may **in the future** discover security issues that were not found during due diligence of such acquired or integrated entities, and it may be difficult to integrate companies into our information technology environment and security program. In addition, our reliance on third ~~- party service providers~~ **parties has in the past and** could **continue to** introduce new cybersecurity risks and vulnerabilities, including supply- chain attacks, and other threats to our business operations. We rely on third **parties** ~~- party service providers and technologies~~ to operate critical business systems to process confidential, proprietary, and sensitive data in a variety of contexts, including, without limitation, cloud-based infrastructure, data center facilities, encryption and authentication technology, employee email, content delivery to customers, and other functions. We also rely on third **parties** ~~- party service providers~~ to provide other products, services and parts, or otherwise to operate our business. Our ability to monitor these third parties' information security practices is limited, and these third parties may not have adequate information security measures in place. If ~~our~~ **the** third ~~- party service providers~~ **parties with whom we work** experience a security incident or other interruption, we could experience adverse consequences. While we may be entitled to damages if ~~our~~ **the** third ~~- party service providers~~ **parties with whom we work** fail to satisfy their privacy or security- related obligations to us, any award may be insufficient to cover our damages, or we may be unable to recover such award. In addition, supply- chain attacks have increased in frequency and severity, and we cannot guarantee that third parties' infrastructure in our supply chain or ~~our~~ **that of the** third ~~- party partners~~ **parties** ~~'~~ **with whom we work** supply chains have not been compromised. If our security measures are compromised, **as has occurred in the past,** our reputation could be damaged; our data, information or intellectual property, or that of our customers, may be destroyed, stolen, or otherwise compromised; our business may be harmed; and we could incur significant liability. We take steps designed to detect and remediate vulnerabilities in our information systems and those of third parties ~~upon~~ **with** whom we ~~rely~~ **work** , but we may not detect or remediate all such vulnerabilities or do so in a timely manner. The threats and techniques used to exploit vulnerabilities change frequently and are often sophisticated in nature, and may be difficult to detect by security tools. Vulnerabilities could be exploited and result in a security incident. We have limited budgetary and human resources for detecting and remediating vulnerabilities and have experienced difficulties in hiring and retaining qualified security personnel, especially after our recent restructuring actions. We may experience delays in developing and deploying remedial measures, including patches, designed to address identified vulnerabilities, and our remedial measures may require action by our customers such as installing patches or updates, which may increase the amount of time a vulnerability remains unremediated. We have not always been able in the past and may be unable in the future to anticipate or prevent threats or techniques used to detect or exploit vulnerabilities in our information systems or third- party software, or obtain unauthorized access to or compromise our systems. In addition, security researchers and other individuals have in the past and will continue in the future to actively search for and exploit actual and potential vulnerabilities in our software or services. This activity may increase because of increased demand for our services and increased media scrutiny of our unified communications and collaboration platform, and can lead to additional adverse publicity, reputational harm, extortion threats, business and operational interruptions, security incidents, additional expenses, litigation, regulatory investigations and actions, and substantial harm to our business, some of which we have experienced. For example, in July 2019, a security researcher published a blog highlighting concerns with the Zoom Meeting platform, including certain video- on features. We were able to release updates to the software addressing these vulnerabilities, and we are not aware of any customers being affected or meetings compromised by these vulnerabilities. In most cases customers are responsible for installing this update to the software, and their software is subject to these vulnerabilities until they do so. Additionally, in March 2020, a security researcher reported certain vulnerabilities related to our macOS version that could have allowed an unauthorized person to gain root access to a user' s system. Given the nature of our business and

operations, our products and services will inevitably contain vulnerabilities or critical security defects that have not been identified or remediated and cannot be disclosed without compromising security. We have identified high or critical vulnerabilities in our products, services and information systems in the past, and we expect that we will continue to identify such vulnerabilities in the future. We cannot be certain that we will be able to address any vulnerabilities in our products, services and information systems that we may become aware of in the future, or there may be delays in developing patches that can be effectively deployed to address vulnerabilities. We will continue to make prioritization decisions based on, among other things, our available resources, the efficacy of our security tools, and the increasing workload to meet certain security obligations, to determine which vulnerabilities or security defects to fix and the timing of these fixes, which could result in an exploit that compromises security. In some cases, customers are responsible for installing our software updates, and until they do so, their service remains subject to the vulnerabilities addressed in the software update. Vulnerabilities and critical security defects, errors in remediating vulnerabilities or security defects, failure of third- party providers to remediate vulnerabilities or security defects, or customers not deploying security releases or deciding not to install software updates could result in claims of liability against us, damage our reputation, or otherwise harm our business. Security incidents and vulnerabilities, and concerns regarding privacy, data protection, and information security may also prevent some of our customers and users from using or cause some of our customers and users to stop using our solutions and fail to upgrade or renew their subscriptions. Failures to meet customers' and users' expectations with respect to security and confidentiality of their data and information could damage our reputation and affect our ability to retain customers and users, attract new customers and users, and grow our business. In addition, cybersecurity events or security vulnerabilities could result in breaches of our agreements with customers, lawsuits against us (including class action litigation), regulatory investigations or actions, and significant increases in costs, including costs for remediating the effects of such an event or vulnerability, lost revenue due to network downtime, and a decrease in customer and user trust, increases in insurance premiums due to cybersecurity incidents, increased costs to address cybersecurity issues, and attempts to prevent future incidents, fines, penalties, judgments and settlements, and attorney fees, and harm to our business and our reputation because of any such incident. Any of the previously identified or similar threats could cause a security incident or other interruption that could result in unauthorized, unlawful, or accidental acquisition, modification, destruction, loss, alteration, encryption, disclosure of, or access to confidential, proprietary, or sensitive data or our information technology systems, or those of the third parties ~~upon~~ **with** whom we **work** ~~rely.~~ A security incident or other interruption could disrupt our ability (and that of third parties ~~upon~~ **with** whom we ~~rely~~ **work** ) to provide our services. We ~~may~~ expend significant resources or modify our business activities to try to protect against security incidents. Additionally, certain privacy, data protection, and information security obligations ~~may~~ require us to implement and maintain ~~specific~~ **certain** security measures or industry- standard or reasonable security measures to protect our information technology systems and sensitive data. Many governments have enacted laws requiring companies to provide notice of data security incidents, including those recently promulgated by the SEC. **These laws may also require us to take certain measures, such as providing credit monitoring to individuals.** Such laws are inconsistent, and compliance in the event of a widespread data breach is costly **, and the disclosure or the failure to comply with such requirements could lead to adverse consequences** . In addition, some of our customers require us to notify them of data security breaches. Actual or perceived security gaps or security compromises experienced in our industry or by our competitors, our customers, a third party ~~upon~~ **with** whom we ~~rely~~ **work** , or us could cause us to experience adverse consequences, such as government enforcement actions (for example, investigations, fines, penalties, audits, and inspections); additional reporting requirements and / or oversight; restrictions on processing sensitive data (including personal information); litigation (including class claims); indemnification obligations; negative publicity; reputational harm; monetary fund diversions; diversion of management attention; interruptions in our operations (including availability of data); financial loss; and other similar harms. Security incidents and attendant consequences may cause customers to stop using our services, deter new customers from using our services, and negatively impact our ability to grow and operate our business. In addition, while more than half of our employees are based in the United States, like many similarly situated technology companies, we have a sizable number of research and development personnel outside of the United States, including in China, which has exposed and could continue to expose us to governmental and regulatory as well as market and media scrutiny regarding the actual or perceived integrity of our platform or data security and privacy features. Increased usage of our services, novel uses of our services, and additional awareness of Zoom and our brand has led and could in the future lead to greater public scrutiny of, press related to, or a negative perception of our information security and potential vulnerabilities associated with our platform. For example, during the COVID- 19 pandemic, we opened our platform to unprecedented numbers of first- time users, leading to challenges for users who did not have full IT support or established protocols for security and privacy like our larger customers. As a result, we have experienced negative publicity related to meeting disruptions and security and privacy issues, including on encryption. Such unfavorable publicity and scrutiny could result in material reputational harm, a loss of customer and user confidence, increased regulatory or litigation exposure, additional expenses, and other harm to our business. There can be no assurance that any limitations of liability provisions in our subscription agreements, terms of use or other agreements would be enforceable or adequate or would otherwise protect us from any such liabilities or damages with respect to any particular claim. We also cannot be sure that our existing general liability insurance coverage and coverage for cyber liability or errors or omissions will continue to be available on acceptable terms or will be available in sufficient amounts to cover one or more large claims or that the insurer will not deny coverage as to any future claim. The successful assertion of one or more large claims against us that are not covered or 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 harm our business. In addition to experiencing a security incident, third parties may gather, collect, or infer sensitive information about us from public sources, data brokers, or other means that reveals competitively sensitive details about our organization and could be used to undermine our competitive advantage or market position. Our business depends on a strong brand, and if we are not

able to maintain and enhance our brand, our ability to expand our base of users will be impaired and our business will be harmed. We believe that maintaining and enhancing the Zoom brand is critical to expanding our base of customers and users and, in particular, conveying to users and the public that the Zoom brand consists of a broad communications and collaboration platform, rather than just one distinct product. For example, if users view the Zoom brand primarily as a video conferencing point solution or utility rather than as a platform that connects people through video, voice, chat and content sharing, or have a negative perception of our privacy and security, then our market position may be detrimentally impacted. We anticipate that, as our market becomes increasingly competitive, maintaining and enhancing our brand may become increasingly difficult and expensive. Any unfavorable publicity or perception of our platform, including from any delays or interruptions in service due to capacity constraints stemming from increased usage, from our privacy or security features, because of sentiment towards the providers of communication and collaboration technologies generally, or from our integration of new product functionalities using technologies with heightened public interest, could adversely affect our reputation and our ability to attract and retain customers. Similarly, any unfavorable perception of our company, including due to any actual or perceived violation by our employees of our policies, such as our Code of Business Conduct and Ethics, could cause us reputational harm and customer loss, impact our financial performance, expose us to litigation, and harm our business, among other things. If we fail to promote and maintain the Zoom brand, including consumer and public perception of our platform or our company, or if we incur excessive expenses in this effort, our business will be harmed. If we fail to manage our growth effectively, our business, financial condition and results of operations may be harmed. While our employee headcount both in the United States and internationally has generally increased over time, we have undertaken, and may undertake from time to time in the future, restructuring actions to better align our financial model ~~and~~ . For example, in February 2023, we commenced certain restructuring actions, designed to reduce operating costs and continue advancing our ongoing commitment to profitable growth. These organizational changes may not achieve or sustain the targeted benefits, or the benefits, even if achieved, may not be adequate to meet our long- term profitability and operational expectations. Steps we take to manage our business operations, including workplace policies for employees, and to align our operations with our strategies for future growth, may adversely affect our reputation and brand, our ability to recruit, retain and motivate highly skilled personnel. Additionally, while we expect to continue to grow our business and operations over time, we have encountered in the past, and may encounter in the future, risks and uncertainties frequently experienced by growing companies in rapidly changing industries. Our ability to manage our growth and business operations effectively and to integrate new employees, technologies and acquisitions into our existing business will require us to continue to expend resources ~~to continue~~ to support our global user- base and to retain, attract, train, motivate and manage employees. This places a continuous, significant strain on our management, operational, and financial resources. If we fail to achieve the necessary level of efficiency in our organization as it grows, or if we are not able to accurately forecast future growth, our business would be harmed. Our ability to sell subscriptions to our platform could be harmed by real or perceived material defects or errors in our platform. The software technology underlying our platform is inherently complex and may contain material defects or errors, particularly when new products are first introduced or when new features or capabilities are released. We have from time to time found defects or errors in our platform, and new defects or errors in our existing platform or new products may be detected in the future by us or our users. There can be no assurance that our existing platform and new products will not contain defects. Any real or perceived errors, failures, vulnerabilities, or bugs in our platform have in the past resulted and could in the future result in negative publicity or lead to data security, access, retention, or other performance issues, all of which could harm our business. The costs incurred in correcting such defects or errors may be substantial and could harm our business. Moreover, the harm to our reputation and legal liability related to such defects or errors may be substantial and would harm our business. We also utilize hardware purchased or leased and software and services licensed from third parties to offer our platform. Any defects in, or unavailability of, our or third- party hardware, software, or services that cause interruptions to the availability of our services, loss of data, or performance issues could, among other things: • cause a reduction in revenue or delay in market acceptance of our platform; • require us to issue refunds to our customers or expose us to claims for damages; • cause us to lose existing customers and make it more difficult to attract new customers; • divert our development resources or require us to make extensive changes to our platform, which would increase our expenses; • increase our technical support costs; and • harm our reputation and brand. If we were to lose the services of our Chief Executive Officer or other members of our senior management team, we may not be able to execute our business strategy. Our success depends in a large part upon the continued service of key members of our senior management team. In particular, our founder, President and Chief Executive Officer, Eric S. Yuan, is critical to our overall management, as well as the continued development of our products, services, the Zoom platform, our culture, our strategic direction, engineering, and our global operations, including regions such as the United States, Europe, Middle East, and Africa (“ EMEA ”), and Asia Pacific (“ APAC ”). All of our executive officers are at- will employees, and we do not maintain any key person life insurance policies. Any changes in our senior management team in particular, even in the ordinary course of business, **including the transition of our Chief Financial Officer in 2024,** may be disruptive to our business. Such changes may result in a loss of institutional knowledge and cause disruptions to our business. If our senior management team fails to work together effectively or execute our plans and strategies on a timely basis as a result of management turnover or otherwise, our business could be harmed. The failure to attract and retain additional qualified personnel or to maintain our happiness- centric company culture could harm our business and culture and prevent us from executing our business strategy. To execute our business strategy, we must attract and retain highly - qualified personnel. Competition for executives, software developers, sales personnel, and other key employees in our industry is intense. In particular, we compete with many other companies for software developers with high levels of experience in designing, developing, and managing software for communication and collaboration technologies, as well as for skilled sales and operations professionals. At times, we have experienced, and we may continue to experience, difficulty in hiring and retaining employees with appropriate qualifications, and we may not be able to fill positions in a timely manner or at

all, which may be exacerbated by our recent restructuring actions and any similar future actions. In addition, our recruiting personnel, methodology, and approach may need to be altered to address a changing candidate pool and profile. We may not be able to identify or implement such changes in a timely manner. In addition, we have experienced and may continue to experience employee turnover as a result of our recent restructuring actions. New hires require training and take time before they achieve full productivity. New employees may not become as productive as we expect, and we may be unable to hire or retain sufficient numbers of qualified individuals. If we fail to attract new personnel or fail to retain and motivate our current personnel, our business could be harmed. Many of the companies with which we compete for experienced personnel have greater resources than we have, and some of these companies may offer more attractive compensation packages. Particularly in the San Francisco Bay Area, job candidates and existing employees carefully consider the value of the equity awards they receive in connection with their employment. If the perceived value of our equity awards declines, or if the mix of equity and cash compensation that we offer is unattractive, it may adversely affect our ability to recruit and retain highly skilled employees. Job candidates may also be threatened with legal action under agreements with their existing employers if we attempt to hire them, which could impact hiring and result in a diversion of our time and resources. Additionally, laws and regulations, such as restrictive immigration laws, may limit our ability to recruit internationally. We must also continue to retain and motivate existing employees through our compensation practices, company culture, and career development opportunities. If we fail to attract new personnel or to retain our current personnel, our business would be harmed. We believe that a critical component to our success and our ability to retain our best people is our culture. As we continue to grow and develop a public company infrastructure, we may find it difficult to maintain our happiness- centric company culture. Transparency is also an important part of our culture, and one that we practice every day. As we continue to grow, maintaining this culture of transparency will present its own challenges that we will need to address, including the type of information and level of detail that we share with our employees. In addition, as our stock price has fluctuated since our initial public offering (" IPO "), employees joining us at different times could have significant disparities in proceeds from sales of our equity in the public markets, which could create disparities in wealth among our employees, which may harm our culture and relations among employees and our business. Further, the volatility of our stock price may make our equity compensation less attractive to current and potential employees, and could contribute to increased turnover or difficulties in hiring. We have significant and expanding operations outside the United States, which may subject us to increased business, regulatory and economic risks that could harm our business. Our platform addresses the communications and collaboration needs of users worldwide, and we see international expansion as a major opportunity. Our revenue from APAC and EMEA collectively represented 28. **2 % and 28.** 7 % **,** and 30. 5 ~~%, and 33. 3~~ % of our revenue for the fiscal years ended January 31, **2025,** 2024, **and** 2023, ~~and 2022,~~ respectively ~~. We plan to add local sales support in further select international markets over time~~ . Our customers include multinational corporations with global users, and we expect to continue to expand our international operations, which includes opening offices in new jurisdictions and providing our platform in additional languages to support the needs of these multinational corporations. Any new markets or countries into which we attempt to allow users to access our services or sell subscriptions to our platform may not be receptive. If we are not able to satisfy certain government- and industry- specific requirements, we have in the past and may in the future experience service outages or other adverse consequences, including interference with our local operations or restrictions on our ability to continue our operations in certain jurisdictions, that would impair our ability to operate or expand further into certain markets. As an example, if local or national Chinese government agencies interfered with or placed restrictions on our research and development operations in China, our ability to design new products, features, and functionality on a timely basis or at all, or our ability to effectively deliver our services, would be adversely impacted as a significant portion of our research and development organization resides in China. In addition, our ability to manage our business and conduct our operations internationally in the future requires considerable management attention and resources and is subject to the particular challenges of supporting a rapidly growing business in an environment of multiple languages, cultures, customs, legal and regulatory systems, alternative dispute systems, and commercial markets. Future international expansion will require investment of significant funds and other resources. We also face risks related to recruiting and retaining talented and capable employees outside the United States, including complying with complex employment- and compensation- related laws, regulations, and practices in these international jurisdictions, and maintaining our company culture across all of our offices. We may also be unable to grant equity compensation to employees in certain countries outside of the United States due to the complexities of local laws and regulations. This may require us to offer equally compelling alternatives to supplement our compensation, such as long- term cash compensation plans or increased short- term cash compensation, in order to continue to attract and retain employees in these jurisdictions. Operating internationally subjects us to new risks and increases risks that we currently face, including risks associated with: • providing our platform and operating our business across a significant distance, in different languages and among different cultures, including the potential need to modify our platform and features to ensure that they are culturally appropriate and relevant in different countries; • compliance with applicable international laws and regulations, including laws and regulations with respect to privacy, information security, telecommunications requirements, data protection, consumer protection, automatic renewals, and unsolicited email, and the risk of penalties to us and individual members of management or employees if our practices are deemed to be out of compliance; • operating in foreign jurisdictions where the government may impede or interrupt our ability to provide our services or develop new products, features, and functionality; • management of an employee base in jurisdictions that may not give us the same employment and retention flexibility as the United States; • operating in jurisdictions that do not protect intellectual property rights to the same extent as the United States and the practical enforcement of such intellectual property rights outside of the United States; • foreign government interference with our intellectual property that resides outside of the United States, such as the risk of changes in foreign laws that could restrict our ability to use our intellectual property outside of the foreign jurisdiction in which we developed it; • integration with partners outside of the United States; • compliance by us and our business partners with anti- corruption laws, import and export

control laws, tariffs, trade barriers, economic sanctions, and other regulatory limitations on our ability to provide our platform in certain international markets; • foreign exchange controls that might require significant lead time in setting up operations in certain geographic territories and might prevent us from repatriating cash earned outside the United States; • political and economic instability and other political tensions between countries in which we do business; • changes in diplomatic and trade relationships, including the continuing deterioration in diplomatic relations between the United States and China, **or deterioration in diplomatic relations between** the **United States and countries with which the United States has traditionally enjoyed close ties and alliances, and the ongoing** ~~conflict~~ **conflicts** ~~in Israel and the surrounding area, and the continuing war~~ between Russia and Ukraine **and in the Middle East** ; • generally longer payment cycles and greater difficulty in collecting accounts receivable, a risk that may increase as a result of recent macroeconomic conditions, such as high inflation, recessionary environments, recent bank failures and related uncertainties, and fluctuations in foreign currency exchange rates, weighing on our customers' ability to pay for our service on a timely basis; • double taxation of our international earnings and potentially adverse tax consequences due to changes in the income and other tax laws of the United States or the international jurisdictions in which we operate, including the imposition of digital services taxes; and • higher costs of doing business internationally, including increased accounting, travel, infrastructure, and legal compliance costs. As described above, following Russia' s military invasion of Ukraine in February 2022, the United States, European Union, and other nations announced various sanctions against Russia and export restrictions against Russia and Belarus. Such restrictions include blocking sanctions on some of the largest state- owned and private Russian financial institutions, and their removal from the Society for Worldwide Interbank Financial Telecommunication, or the SWIFT, payment system. The invasion of Ukraine and the retaliatory measures that have been taken, and could be taken in future, by the United States, NATO, and other countries have created global security concerns that could result in a regional conflict and otherwise have a lasting impact on regional and global economies, any or all of which could adversely affect our business, including preventing us from performing existing contracts, pursuing new business opportunities, or receiving payments for services already provided to customers. Compliance with laws and regulations applicable to our global operations substantially increases our cost of doing business in international jurisdictions. We may be unable to keep current with changes in laws and regulations as they occur. Although we have implemented policies and procedures designed to support compliance with these laws and regulations, there can be no assurance that we will always maintain compliance or that all of our employees, contractors, partners, and agents will comply. In addition, legal requirements in the United States and other countries may come into conflict with each other making it challenging or impossible to comply with both countries' legal requirements simultaneously. Any violations could result in enforcement actions, fines, civil and criminal penalties, damages, injunctions, or reputational harm. If we are unable to comply with these laws and regulations or manage the complexity of our global operations successfully, we may need to relocate or cease operations in certain foreign jurisdictions. We are subject to various U. S. and international anti- corruption laws, and any failure to comply with such laws could harm our business, financial condition, and results of operations. We are subject to various U. S. and international anti- corruption laws, such as the U. S. Foreign Corrupt Practices Act of 1977, as amended (the " FCPA "), and the U. K. Bribery Act 2010, as well as other similar anti- bribery and anti- kickback laws and regulations. These laws and regulations generally prohibit companies and their employees and intermediaries, from directly or indirectly authorizing, offering, or providing improper payments or benefits to government officials and other recipients for improper purposes. The FCPA also requires public companies to make and keep books and records that accurately and fairly reflect the transactions of the corporation and to devise and maintain an adequate system of internal accounting controls. Although we take precautions to prevent violations of anti- corruption laws, our exposure for violating these laws increases as we continue to expand our international presence, and any failure to comply with such laws could harm our business, financial condition, and results of operations. Geopolitical tension between the United States and China, or between other ~~countries~~ **economies** , such as Taiwan, and China, may intensify and lead to increased scrutiny of our business operations in China. We have a significant number of employees, primarily engineers, in China, where personnel costs are less expensive than in many other geographies. The number or proportion of our employees in China has fluctuated in the past and may fluctuate in the future due to a number of factors, including macroeconomic changes and internal restructuring. Geopolitical and national security tensions between the United States and China, or between other countries and China, have in the past, currently are and could in the future lead to increased scrutiny of our business operations in China and a negative perception among current and potential customers regarding our collection, use, storage, disclosure, and processing of personal information, and our privacy policies, any of which may harm our reputation and business. Additionally, we may face certain adverse consequences, as a result of geopolitical and national security tensions between the United States and China, including interference with, or restrictions on, our local operations that would impair our ability to operate in China. As an example, if local or national Chinese government agencies interfered with or placed restrictions on our research and development operations in China, our ability to design new products, features, and functionality on a timely basis or at all, or our ability to effectively deliver our service, would be adversely impacted as a significant portion of our research and development organization resides in China. In June and July 2020, we received subpoenas from the Department of Justice' s U. S. Attorney' s Office for the Eastern District of New York (" EDNY ") and the Department of Justice' s U. S. Attorney' s Office for the Northern District of California (" NDCA "). The EDNY and NDCA subpoenas requested information about (among other things) our interactions with foreign governments and / or foreign political parties, including the Chinese government, as well as about storage of and access to user data, including the use of servers based overseas. In addition, the EDNY subpoena requested information about the actions we took responding to law enforcement requests from the Chinese government. The NDCA subpoena also requested documents and information about (among other things) contacts between our employees and representatives of the Chinese government, and any attempted or successful influence by any foreign government in our policies, procedures, practices, and actions as they relate to users in the United States. We are fully cooperating with these investigations and have **conducted** ~~been conducting~~ our own thorough internal investigation. These investigations are ongoing,

and we do not know when they will be completed, which facts we will ultimately discover as a result of the investigations, or what actions the government may or may not take. We cannot predict the outcome of these investigations, and a negative outcome in any or all of these matters could cause us to incur substantial fines, penalties, or other financial exposure, as well as material reputational harm, a loss of customer and user confidence and business, additional expenses, and other harm to our business. We recognize revenue from subscriptions to our platform over the terms of these subscriptions. Consequently, increases or decreases in new sales may not be immediately reflected in our results of operations and may be difficult to discern. We recognize revenue from subscriptions to our platform over the terms of these subscriptions. As a result, a portion of the revenue we report in each quarter is derived from the recognition of deferred revenue relating to subscriptions entered into during previous quarters. Consequently, a decline in new or renewed subscriptions in any single quarter may have an immaterial impact on the revenue that we recognize for that quarter. However, such a decline will negatively affect our revenue in future quarters. Accordingly, the effect of significant downturns in sales and potential changes in our pricing policies or rate of customer expansion or retention may not be fully reflected in our results of operations until future periods. In addition, a significant portion of our costs is expensed as incurred, while revenue is recognized over the term of the subscription. As a result, growth in the number of new customers and users could continue to result in our recognition of higher costs and lower revenue in the earlier periods of our subscriptions. Finally, our subscription- based revenue model also makes it difficult for us to rapidly increase our revenue through additional sales in any period, as revenue from new customers or from existing customers ~~that~~ **who** increase their use of our platform or upgrade to a higher- priced plan must be recognized over the applicable subscription term. Any failure to offer high- quality support for our customers and users may harm our relationships with our customers and users and, consequently, our business. Increased user demand for support may result in increased costs that may harm our results of operations. For example, during the COVID- 19 pandemic we saw surging demand requiring us to allocate additional resources to support our expanded customer and user base, including many who were using our platform for the first time, placing additional pressure on our support organization. In addition, as we continue to support our global user base, we need to be able to continue to provide efficient support that meets our customers and users' needs globally at scale. If we are unable to provide efficient user support globally at scale or if we need to hire additional support personnel, our business may be harmed. Our new customer signups are highly dependent on our business reputation and on recommendations from our existing customers and users. Any failure to maintain high- quality support, or a market perception that we do not maintain high- quality support for our customers and users, would harm our business. We utilize our network of resellers to sell our products and services, and our failure to effectively develop, manage, and maintain our indirect sales channels would harm our business. Our future success depends on our continued ability to establish and maintain a network of channel relationships, and we expect that we will need to maintain and expand our network as we expand into international markets. A small portion of our revenue is derived from our network of sales agents and resellers, which we refer to collectively as resellers, many of which sell or may in the future decide to sell their own products and services or services from other communications solutions providers. Loss of or reduction in sales through these third parties could reduce our revenue. Our competitors may in some cases be effective in causing our resellers or potential resellers to favor their products and services or prevent or reduce sales of our products and services. Recruiting and retaining qualified resellers in our network and training them in our technology, product offerings and processes requires significant time and resources. For resellers in certain emerging markets, we may be unable to effectively oversee and quality check certain processes, such as customer due diligence, which has and may continue to impact such resellers' ability to implement robust customer verification protocols and mitigate fraud risk. If we decide to further develop and expand our indirect sales channels, we must continue to scale and improve our processes and procedures to support these channels, including investment in systems and training. Many resellers may not be willing to invest the time and resources required to train their staff to effectively sell our platform. If we fail to maintain relationships with our resellers, develop relationships with new resellers in new markets, expand the number of resellers in existing markets, or manage, train, or provide appropriate incentives to our existing resellers, our ability to increase the number of new customers and increase sales to existing customers could be adversely impacted, which would harm our business. Our results of operations, which are reported in U. S. dollars, could be adversely affected if currency exchange rates fluctuate substantially in the future. We sell to customers globally and have international operations primarily in Australia, China, and the U. K. As we continue to expand our international operations, we will become more exposed to the effects of fluctuations in currency exchange rates. Although the majority of our cash generated from revenue is denominated in U. S. dollars, a portion of our revenue is denominated in foreign currencies, and our expenses are generally denominated in the currencies of the jurisdictions in which we conduct our operations. For the fiscal years ended January 31, **2025,** 2024, **and** 2023 ~~, and 2022~~ , 19. 3 %, **19. 3 %, and** 20. 0 % **of our revenue** , **respectively,** and ~~22~~ **16** . ~~6~~ **4** % ~~of our revenue~~ , ~~respectively, and~~ 13. 7 %, **and** 10 ~~. 8 %, and 16~~ . 8 % of our expenses, respectively, were denominated in currencies other than U. S. dollars. Because we conduct business in currencies other than U. S. dollars but report our results of operations in U. S. dollars, we also face remeasurement exposure to fluctuations in currency exchange rates, which could hinder our ability to predict our future results and earnings and could materially impact our results of operations. For example, for the fiscal year ended January 31, ~~2024~~ **2025** , our total revenue was lower than anticipated in part due to the strengthening of the U. S. dollar. We do not currently maintain a program to hedge exposures to non- U. S. dollar currencies. Our sales to government entities and other government contractors are subject to a number of additional challenges and risks. We expect to continue selling our products and services to U. S. federal and state and foreign governmental agency customers, which may occur through sales to other companies that re- sell our services to government customers and / or through direct sales to government entities. While we are a U. S. Federal Risk and Authorization Management Program (" FedRAMP ") authorized SaaS service, selling to government entities and other government contractors presents a number of unique challenges and risks including the following: • selling to governmental entities can be more competitive, expensive, and time- consuming than selling to private entities, often requiring significant up- front time and expense and ongoing compliance costs without any

assurance that these efforts will generate a sale; • **contracts with governmental entities are subject to termination for the convenience of the customer; •** government certification requirements may change, or we may be unable to achieve or sustain one or more government certifications, including FedRAMP, which may restrict our ability to sell into the government sector until we have attained such certificates; • contracts with governmental entities and other government contractors, including resellers in the government market, contain terms that are less favorable than what we generally agree to in our standard agreements, including, terms and conditions required by regulation that are not negotiable with the customer; • non- compliance with terms and conditions of government contracts, or with representations or certifications made in connection with government contracts, can result in significantly more adverse consequences than we typically would expect in the commercial market, including, depending on the circumstances, criminal liability, liability under the civil False Claims Act, and / or suspension or debarment from doing business with governmental entities; **• as a U. S. government contractor, we may be subject to executive orders and regulatory changes affecting various aspects of our operations, including compliance with nondiscrimination plans, and any required elimination or modification of such plans in response to new executive orders could pose challenges in hiring or retaining employees and may lead to other adverse operational impacts, while failure to comply with these requirements could expose us to administrative, civil, or criminal liabilities, including fines, penalties, repayments or suspension or debarment from eligibility for future U. S. government contracts;** and • government demand and payment for our products may be influenced, among other things, by public sector budgetary cycles and funding authorizations, with funding reductions or delays having an adverse impact on public sector demand for our products. To the extent that we become more reliant on contracts with government entities and / or other government contractors in the future, our exposure to such risks and challenges could increase, which in turn could adversely impact our business. In May 2021, the Biden Administration issued an Executive Order requiring federal agencies to implement additional information technology security measures, including, among other things, requiring agencies to adopt multifactor authentication and encryption for data at rest and in transit to the maximum extent consistent with Federal records laws and other applicable laws. The Executive Order will lead to the development of secure software development practices and / or criteria for a consumer software labeling program, which will reflect a baseline level of secure practices, for software that is developed and sold to the U. S. federal government. Software developers will be required to provide visibility into their software and make security data publicly available. Due to this Executive Order, federal agencies may require us to modify our cybersecurity practices and policies, thereby increasing our compliance costs. If we are unable to meet the requirements of the Executive Order, our ability to work with the U. S. government may be impaired and may result in a loss of revenue **. In January 2025, the current administration began issuing Executive Orders identifying new government policy and directing U. S. federal agencies to evaluate their current actions, including certain spending, to ensure that such actions are consistent with new Administration priorities. Some of those Executive Orders are the subjects of pending litigation, and there remains significant uncertainty about the ways in which agencies will implement the new Executive Orders. Such implementation could negatively affect our current and future business with U. S. government agencies** . Our current platform, as well as products, features, and functionality that we may introduce in the future, may not be widely accepted by our customers and users or may receive negative attention or may require us to compensate or reimburse third parties, any of which may lower our margins and harm our business. Our ability to engage, retain, and increase our base of customers and users and to increase our revenue will depend on our ability to successfully create new products, features, and functionality, both independently and together with third parties. We may introduce significant changes to our existing platform or develop and introduce new and unproven products, including technologies with which we have little or no prior development or operating experience. These new products and updates may not perform as expected, have attracted and may in the future attract negative attention if they involve technologies with heightened public interest, may fail to engage, retain, and increase our base of customers and users or may create lag in adoption of such new products. New products may initially suffer from performance and quality issues that may negatively impact our ability to market and sell such products to new and existing customers. The short- and long- term impact of any major change to our products, or the introduction of new products, is particularly difficult to predict. If new or enhanced products **, including those incorporating AI features,** fail to engage, retain, and increase our base of customers, or do not perform as expected, we may fail to generate sufficient revenue, operating margin, or other value to justify our investments in such products, any of which may harm our business in the short term, long term, or both. In addition, our current platform, as well as products, features, and functionality that we may introduce in the future, may require us to compensate or reimburse third parties. For example, our cloud phone system, Zoom Phone, is a PBX phone solution that requires us to compensate carriers that operate the PSTN. As a result, a portion of the payments that we will receive from customers ~~that~~ **who** will use our Zoom Phone product will be allocated towards compensating these telephone carriers, which lowers our margins for Zoom Phone as compared to our other products. In addition, new products that we introduce in the future may similarly require us to compensate or reimburse third parties, all of which would lower our profit margins for any such new products. If this trend continues with our new and existing products, including Zoom Phone, it could harm our business. If we experience excessive fraudulent activity or cannot meet evolving credit card association merchant standards, we could incur substantial costs and lose the right to accept credit cards for payment, which could cause our customer and paid user base to decline significantly. A large portion of our customers authorize us to bill their credit card accounts directly for our products. If customers pay for their subscriptions with stolen credit cards, we could incur substantial third- party vendor costs for which we may not be reimbursed. Further, our customers provide us with credit card billing information online or over the phone, and we do not review the physical credit cards used in these transactions, which increases our risk of exposure to fraudulent activity. We also incur charges, which we refer to as chargebacks, from the credit card companies for claims that the customer did not authorize the credit card transaction for our products, something that we have experienced in the past. If the number of claims of unauthorized credit card transactions becomes excessive, we could be assessed substantial fines for excess chargebacks, and we could lose the

right to accept credit cards for payment. In addition, credit card issuers may change merchant standards, including data protection and documentation standards, required to utilize their services from time to time. If we fail to maintain compliance with current merchant standards or fail to meet new standards, the credit card associations could fine us or terminate their agreements with us, and we would be unable to accept credit cards as payment for our products. Our products may also be subject to fraudulent usage and schemes, including third parties accessing customer accounts or viewing and recording data from our communications solutions. These fraudulent activities can result in unauthorized access to customer accounts and data, unauthorized use of our products, and charges and expenses to customers for fraudulent usage. We may be required to pay for these charges and expenses with no reimbursement from the customer, and our reputation may be harmed if our products are subject to fraudulent usage. Although we implement multiple fraud prevention and detection controls, we cannot assure you that these controls will be adequate to protect against fraud. Substantial losses due to fraud or our inability to accept credit card payments would cause our customer base to significantly decrease and would harm our business. We may have exposure to greater than anticipated tax liabilities, which could harm our business. We are subject to income taxes in the United States and various jurisdictions outside of the United States. Our effective tax rate could fluctuate due to changes in the proportion of our earnings and losses in countries with differing statutory tax rates. Our tax expense could also be impacted by changes in non-deductible expenses; changes in tax benefits of stock- based compensation expense; changes in the valuation of, or our ability to use, deferred tax assets; the applicability of withholding taxes; and effects from acquisitions. The provision for taxes on our consolidated financial statements could also be impacted by changes in accounting principles, changes in U. S. federal, state, or foreign tax laws applicable to corporate multinationals, other fundamental changes in tax law currently being considered by many countries, and changes in taxing jurisdictions' administrative interpretations, decisions, policies, and positions. In addition, we are subject to review and audit by U. S. federal, state, local, and foreign tax authorities. Such tax authorities may disagree with tax positions we take, and if any such tax authority were to successfully challenge any such position, our business could be adversely impacted. The Tax Cuts and Jobs Act of 2017 requires the capitalization and amortization of research and development expenses effective for years beginning after December 31, 2021. The mandatory capitalization requirement increased our cash tax liabilities but also decreased our effective tax rate due to increasing the foreign- derived intangible income deduction. Although Congress ~~is~~ **has been** considering legislation that would defer the amortization requirement to later years, we have no assurance that the provision will be repealed or otherwise modified. Absent a change in legislation, we expect the mandatory capitalization requirement will continue to have a material impact on our cash flows. We may also be subject to additional tax liabilities due to changes in non- income- based taxes resulting from changes in U. S. federal, state, local, or foreign tax laws; changes in taxing jurisdictions' administrative interpretations, decisions, policies, and positions; results of tax examinations, settlements, or judicial decisions; changes in accounting principles, changes to our business operations, including acquisitions; as well as the evaluation of new information that results in a change to a tax position taken in a prior period. Further, the Organization for Economic Cooperation and Development (" OECD ") and the Inclusive Framework of G20 and other countries have issued proposals related to the taxation of the digital economy. In addition, several countries have proposed or enacted Digital Services Taxes (" DST "), many of which would apply to revenue derived from **certain** digital services. Future developments related to such proposals, in particular any unilateral actions outside of the OECD' s Inclusive Framework such as the imposition of DST rules, could have an adverse impact on our business by increasing our future tax obligations. The OECD has also been working on a Base Erosion and Profits Shifting project that, upon implementation, would change various aspects of the existing framework under which our tax obligations are determined in many of the countries in which we operate. In this regard, the OECD has proposed policies aiming to modernize global tax systems, including a country- by- country 15 % minimum effective tax rate (" Pillar Two ") for multinational companies. Numerous countries have enacted, or are in the process of enacting, legislation to implement the Pillar Two model rules with a subset of the rules becoming effective during our fiscal year ~~ending~~ **ended** January 31, 2025, and the remaining rules becoming effective for our fiscal year ending January 31, 2026, or in later periods ~~. At this point in time, we do not expect material tax impacts associated with Pillar Two rules in the countries where we operate for the fiscal year ending January 31, 2025~~. As these rules continue to evolve with new legislation and guidance, we will continue to monitor and account for the enactment of Pillar Two rules in the countries where we operate, and the potential impacts such rules may have on our effective tax rate and cash flows in future years. We have acquired and may continue to acquire other businesses or receive offers to be acquired, which could require significant management attention, disrupt our business, or dilute stockholder value. We have made and may continue in the future to make acquisitions of other companies, products, and technologies. We have limited experience in acquisitions. We may not be able to find suitable acquisition candidates and we may not be able to complete acquisitions on favorable terms, if at all, due to, among other things, possible delays and challenges in obtaining regulatory approvals. If we do complete acquisitions, we may not ultimately strengthen our competitive position or achieve our goals, and any acquisitions we complete could be viewed negatively by users, developers, or investors. In addition, we may not be able to integrate acquired businesses successfully or effectively manage the combined company following an acquisition. If we fail to successfully integrate our acquisitions, or the people or technologies associated with those acquisitions, into our company, the results of operations of the combined company could be adversely affected. The process of acquiring a business, including any integration efforts, requires significant time and resources, requires significant attention from management, and can disrupt the ordinary functioning of our business, and we may not be able to manage the process successfully, which could harm our business. In addition, we may not successfully evaluate or utilize the acquired technology and accurately forecast the financial impact of an acquisition transaction, including accounting charges. We may have to pay cash, incur debt, or issue equity securities to pay for any such acquisition, each of which could affect our financial condition or the value of our capital stock. The sale of equity to finance any such acquisitions could result in dilution to our stockholders. If we incur more debt, it would result in increased fixed obligations and could also subject us to covenants or other restrictions that would impede our ability to flexibly operate our business. We have a limited operating history at the

current scale of our business, which makes it difficult to evaluate our prospects and future results of operations. During fiscal year 2021, we experienced rapid growth in usage of our unified communications and collaboration platform largely due to the COVID- 19 pandemic. This usage dramatically changed the scale of our business, and we have a limited operating history at the current scale of our business. As a result, our ability to forecast our future results of operations is limited and subject to a number of uncertainties, including our ability to plan for and model future growth and expenses. Our historical revenue growth should not be considered indicative of our future performance. Further, in future periods, our revenue growth could continue to slow or our revenue could decline for a number of reasons, including any reduction in demand for our platform; increased competition; contraction of our overall market; our inability to accurately forecast demand for our platform and plan for capacity constraints; or our failure, for any reason, to capitalize on growth opportunities or to adapt and respond to inflationary factors affecting our business or future economic recession. The changes the COVID- 19 pandemic fostered on the way companies operate, including the shifts to remote and hybrid work have limited our ability to forecast revenue, costs, and expenses due to the uncertainty around how companies choose to operate in the future, including the impacts of a remote and hybrid workplace. We have encountered and will encounter risks and uncertainties frequently experienced by growing companies in rapidly changing industries, such as the risks and uncertainties described herein. If our assumptions regarding these risks and uncertainties, which we use to plan our business, are incorrect or change, or if we do not address these risks successfully, our business would be harmed. We rely on data from tools to calculate certain of our key business metrics. Real or perceived inaccuracies in such metrics may harm our reputation and negatively affect our business. We track our key business metrics with tools that are not independently verified by any third party. Our tools have limitations, and our methodologies for tracking these metrics may change over time, which could result in unexpected changes to our performance metrics, including the key metrics we report. If the tools we use to track these metrics over- or undercount performance or contain errors, the data we report may not be accurate and our understanding of certain details of our business may be distorted, which could affect our longer- term strategies. We are continually seeking to improve our ability to measure our key business metrics, and regularly review our processes to assess potential improvements. Risks Related to Laws and Regulations The actual or perceived failure by us, our customers, partners or vendors to comply with stringent and evolving laws and regulations, industry standards, policies, and contractual obligations relating to privacy, data protection, information security, and other matters could harm **, and has in the past harmed,** our reputation and business and subject us to significant fines and liability. In the ordinary course of business, we collect, receive, store, process, generate, use, transfer, disclose, make accessible, protect, secure, dispose of, transmit, and share confidential, proprietary, and sensitive information, including personal ~~data~~ **information** , customer and user content, business data, trade secrets, intellectual property, third- party data, business plans, transactions, **and** financial information **.** Our data processing activities subject us to numerous privacy, data protection, and information security obligations, such as various laws, regulations, guidance, industry standards, external and internal privacy and security policies, and contractual requirements. Laws in the United States In the United States, federal, state, and local governments have enacted numerous privacy, data protection, and information security laws, including data breach notification laws, personal ~~data~~ **information** privacy laws, consumer protection laws (e. g., Section 5 of the Federal Trade Commission Act), and other similar laws (e. g., wiretapping laws). **Numerous U. S. states have enacted comprehensive privacy laws that impose certain obligations on covered businesses, including providing specific disclosures in privacy notices and affording residents with certain rights concerning their personal data. As applicable, such rights may include the right to access, correct, or delete certain personal data, and to opt- out of certain data processing activities, such as targeted advertising, profiling, and automated decision- making. The exercise of these rights may impact our business and ability to provide our products and services. Certain states also impose stricter requirements for processing certain personal data, including sensitive information, such as conducting data privacy impact assessments. These state laws allow for statutory fines for noncompliance.** For example, the California Consumer Privacy Act of 2018 ~~, as amended by the California Privacy Rights Act of 2020~~ ( ~~" CPRA ") (collectively,~~ " CCPA ") applies to personal information of consumers, business representatives, and employees, and requires businesses to provide specific disclosures in privacy notices and honor requests of California residents to exercise certain privacy rights ~~, such as those noted below~~ . The CCPA provides for fines ~~of up to $ 7, 500 per intentional violation~~ and allows private litigants affected by certain data breaches to recover significant statutory damages. Similar laws are being considered in several other states, as well as at the federal and local levels and we expect more states to pass similar laws in the future. These developments may further complicate compliance efforts and increase legal risk and compliance costs for us and the third parties upon whom we rely. Under various laws and other obligations related to privacy, data protection, and information security, we **are** ~~may be~~ required to obtain certain consents to process personal information. For example, some of our data processing practices may be challenged under wiretapping laws ~~if~~ **when** we obtain consumer information from third parties through various methods, including chatbot and session replay providers, or via third- party marketing pixels. These practices **are** ~~may be~~ subject to increased challenges by class action plaintiffs **. Several states and foreign jurisdictions have enacted statutes imposing obligations on businesses collecting or processing biometric information. For example, Illinois' Biometric Information Privacy Act (" BIPA ") regulates the collection, use, safeguarding, and storage of biometric information and provides for substantial penalties and statutory damages. The Federal Trade Commission (" FTC "), has indicated that use of biometric technologies (including facial recognition technologies) may be subject to additional scrutiny** . Our inability or failure to obtain consent for these practices could result in adverse consequences, including class action litigation ~~and~~ **,** mass arbitration demands **, and regulatory attention** . Laws Outside of the United States Outside the United States, an increasing number of laws, regulations, and industry standards related to privacy, data protection, and information security may govern. For example, the European Union' s General Data Protection Regulation (" EU GDPR "), the United Kingdom' s GDPR (" UK GDPR "), Brazil' s General Data Protection Law (Lei Geral de Proteção de Dados Pessoais, or " LGPD ") (Law No. 13, 709 / 2018), and China' s Personal Information Protection Law (" PIPL ") impose strict requirements for processing personal

information. For example, under the EU GDPR, companies may face temporary or definitive bans on data processing and other corrective actions; fines of up to 20 million Euros under the EU GDPR and 17. 5 million pounds sterling under the UK GDPR, or 4 % of annual global revenue, in each case, whichever is greater; or private litigation related to processing of personal information brought by classes of data subjects or consumer protection organizations authorized at law to represent their interests. **China' s PIPL imposes a set of specific obligations on covered businesses in connection with their processing and transfer of personal information and imposes fines of up to RMB 50 million or 5 % of the prior year' s total annual revenue of the violator.** The Swiss Federal Act on Data Protection (" FADP "), also applies to the collection and processing of personal information, including health- related information, by companies located in Switzerland, or in certain circumstances, by companies located outside of Switzerland. ~~The FADP has been revised and adopted by the Swiss Parliament. Companies must comply with the revised version of the FADP and its revised ordinances from September 1, 2023, which may result in an increase of costs of compliance, risks of noncompliance and penalties for noncompliance.~~ We also ~~target~~ **market to** customers in Asia and have operations in Japan, Singapore and India, and may be subject to new and emerging privacy, data protection, and information security regimes in the region, including Japan' s Act on the Protection of Personal Information, Singapore' s Personal Data Protection Act, and India' s new privacy legislation, the Digital Personal Data Protection Act. In addition, we may be unable to transfer personal information from Europe and other jurisdictions to the United States or other countries due to data localization requirements or limitations on cross- border data flows. Europe and other jurisdictions have enacted laws requiring data to be localized or limiting the transfer of personal information to other countries. In particular, the European Economic Area (" EEA ") and the United Kingdom (" UK ") have significantly restricted the transfer of personal information to the United States and other countries whose privacy laws they generally believe are inadequate. Other jurisdictions **have in the past and** may **continue to** adopt similarly stringent ~~interpretations of their~~ data localization and cross- border data transfer laws. Although there are currently various mechanisms that may be used to transfer personal information from the EEA and UK to the United States in compliance with law, such as the EEA' s standard contractual clause, and the EU- U. S. Data Privacy Framework and the UK extension thereto (which allow for transfers to relevant U. S.- based organizations who self- certify compliance and participate in the Framework), these mechanisms can be subject to legal challenges, and there is no assurance that we can satisfy or rely on these measures to lawfully transfer personal information to the United States. If there is no lawful manner for us to transfer personal information from the EEA, the UK, or other jurisdictions to the United States, or if the requirements for a legally- compliant transfer are too onerous, we could face significant adverse consequences, including the interruption or degradation of our operations, the need to relocate part of or all of our business or data processing activities to other jurisdictions at significant expense, increased exposure to regulatory actions, substantial fines and penalties, the inability to transfer data and work with partners, vendors and other third parties, and injunctions against our processing or transferring of personal information necessary to operate our business. Additionally, companies that transfer personal information out of the EEA and UK to other jurisdictions, particularly to the United States, are subject to increased scrutiny from regulators, individual litigants, and activist groups. Some European regulators have ordered certain companies to suspend or permanently cease certain transfers of personal information out of Europe for allegedly violating the EU GDPR' s cross- border data transfer limitations. For example, in May 2023, the Irish Data Protection Commission determined that a major social media company' s use of the standard contractual clauses to transfer personal information from Europe to the United States was insufficient and levied a 1. 2 billion Euro fine against the company and prohibited the company from transferring personal information to the United States. **The United States is also increasingly scrutinizing certain data transfers and may also impose certain data localization requirements. We may also become subject to new laws that regulate non- personal information. For example, the European Union' s Data Act imposes certain data and cloud service interoperability and switching obligations to enable users to switch between cloud service providers without undue delay or cost, as well as certain requirements concerning cross- border international transfers of, and governmental access to, non- personal information outside the EEA. Depending on how this Act and any similar laws are implemented and interpreted, we may have to adapt our business practices, contractual arrangements, and products and services to comply with such obligations.** Artificial Intelligence Our development and use of AI ~~and machine learning (" ML ")~~ technologies is subject to privacy, data protection, IP, and information security laws, industry standards, external and internal privacy and security policies, and contractual requirements, as well as increasing regulation and scrutiny. Several jurisdictions around the globe, including the EU, the UK and certain U. S. states, have proposed, enacted, or are considering laws governing the development and use of **technology featuring** AI ~~/ ML~~. ~~In~~ **For example,** the EU **' s AI** ~~, regulators have reached political agreement on the text of the Artificial Intelligence~~ Act **enters** ~~, which, when adopted and~~ in ~~force,~~ **phases this year and** will have a direct effect across all EU jurisdictions **. The EU AI Act** and **other similar laws, if implemented and if applicable,** could impose onerous obligations related to the use of AI- related systems. Obligations on AI ~~/ ML~~ may make it harder for us to conduct our business using, or build products incorporating, AI ~~/ ML~~, require us to change our business practices, require us to retrain our algorithms, **require us to disclose or provide greater transparency regarding the nature of our AI tools and the data we have employed to train them,** or prevent or limit our use of AI ~~/ ML~~. For example, the FTC has required other companies to turn over (or disgorge) valuable insights or trainings generated through the use of AI ~~/ ML~~ where they allege the company has violated privacy and consumer protection laws. Additionally, certain privacy laws extend rights to consumers (such as the right to delete certain personal information) and regulate automated decision making, which may be incompatible with our use of AI ~~/ ML~~. If we do not develop or incorporate AI ~~/ ML~~ in a manner consistent with these factors, and consistent with customer expectations, it **has in the past and** may **in the future** result in an adverse impact to our reputation, our business may be less efficient, or we may be at a competitive disadvantage. Similarly, if customers and users do not widely adopt our new product AI ~~/ ML~~ experiences, features, and capabilities, or they do not perform as expected, we may not be able to realize a return on our investment. Laws Relating to Minors Additionally, regulators are increasingly scrutinizing companies that process minors' data and / or provide online

services or other interactive platforms used by minors. Numerous laws, regulations, and legally- binding codes, such as the Children' s Online Privacy Protection Act (" COPPA "), California' s Age Appropriate Design Code, the CCPA, other U. S. state comprehensive privacy laws, the EU and UK GDPR, the EU' s Digital Services Act (" DSA"), the UK' s Online Safety Act (" OSA") and the UK Age Appropriate Design Code, impose various obligations on companies that process minors' data and / or provide online services, or other interactive platforms used by children, including prohibiting showing minors advertising, requiring age verification, limiting the use of minors' personal information, requiring certain consents to process such data and extending certain rights to children and their parents with respect to that data. These laws may, ~~or~~ **and** in some cases already have been subject to legal challenges and changing interpretations which may further complicate our efforts to comply with laws applicable to us. Some of these obligations have wide ranging applications, including for services that do not intentionally target child users (defined in some circumstances as a user under the age of 18 years old). In particular, COPPA is a U. S. Federal law that applies to operators of commercial websites and online services directed to U. S. children under the age of 13 that collect personal information from children, and to operators of general audience websites with actual knowledge that they are collecting personal information from U. S. children under the age of 13. We provide video communications and collaboration services to schools, school districts, and school systems to support traditional, virtual, and hybrid classrooms, distance learning, educational office hours, guest lectures, and other services. As part of these services, Zoom may be used by students, including students under the age of 13, and we collect personal information from such students on behalf of our school subscribers. School subscribers must contractually consent to Zoom' s information practices on behalf of students, prior to students using the services. If we fail to accurately anticipate the application, interpretation, or legislative expansion of these laws, regulations, and legally- binding codes, we could be subject to governmental enforcement actions, data processing restrictions, litigation, fines and penalties, adverse publicity or loss of customers. Moreover, as a result of any such failures, we could be in breach of our K-12 school customer contracts, and our customers could lose trust in us, which could harm our reputation and business. Consumer Preferences and Protection Individuals are increasingly resistant to the collection, use, and sharing of personal information to deliver targeted advertising. Third- party platforms have introduced (or plan to introduce) measures to provide users with more privacy controls over targeted advertising activities, and regulators (including in the EEA / UK) are heavily scrutinizing the use of technologies used to deliver such advertisements. Major technology platforms on which we rely to gather information about consumers have adopted or proposed measures to provide consumers with additional control over the collection, use, and sharing of their personal information for targeted advertising or other purposes. For example, in 2021, Apple began allowing users to more easily opt- out of activity tracking across devices. In February 2022, Google announced similar plans to adopt additional privacy controls on its Android devices to allow users to limit sharing of their data with third parties and reduce cross- device tracking for advertising purposes. Additionally, Google has announced that it intends to phase out third- party cookies in its Chrome browser, which could make it more difficult for us to target advertisements. Other browsers, such as Firefox and Safari, have already adopted similar measures. In addition, legislative proposals and present laws and regulations regulate the use of cookies and other tracking technologies, electronic communications, and marketing. For example, in the EEA and the UK, regulators are increasingly focusing on compliance with requirements related to the targeted advertising ecosystem. European regulators have issued significant fines in certain circumstances where the regulators alleged that appropriate consent was not obtained in connection with targeted advertising activities. In the EU, it is anticipated that the ePrivacy Regulation and national implementing laws will replace the current national laws implementing the ePrivacy Directive, which may require us to make significant operational changes. In the United States, the CCPA, for example, grants California residents the right to opt- out of a company' s sharing of personal information for advertising purposes in exchange for money or other valuable consideration, and requires covered businesses to honor user- enabled browser signals from the Global Privacy Control. Partially as a result of these developments, individuals are becoming increasingly resistant to the collection, use, and sharing of personal information to deliver targeted advertising or other types of tracking. Individuals are now more aware of options related to consent, " do not track " mechanisms (such as browser signals from the Global Privacy Control), and " ad-blocking " software to prevent the collection of their personal information for targeted advertising purposes. As a result, we may be required to change the way we market our products, and any of these developments or changes could materially impair our ability to reach new or existing customers or otherwise negatively affect our operations. We are also subject to consumer protection laws that may affect our sales and marketing efforts, including laws related to subscriptions, billing, and auto-renewal. These laws, as well as any changes in these laws, could adversely affect our self- serve model and make it more difficult for us to retain and upgrade customers and attract new customers. **For example, in September 2024, the FCC adopted new rules scheduled to take effect in 2027 that require video conferencing services to include features that expand accessibility requirements for consumers of our products and services.** Additionally, we have in the past, are currently, and may from time to time in the future become the subject of inquiries and other actions by regulatory authorities as a result of our business practices, including our subscription, billing, and auto- renewal policies. Consumer protection laws may be interpreted or applied by regulatory authorities in a manner that could require us to make changes to our operations or incur fines, penalties, or settlement expenses, which may result in harm to our business. Industry Standards In addition to privacy, data protection and information security laws, we are contractually subject to **certain** industry standards adopted by industry groups and may become subject to **additional** such obligations in the future. We ~~may~~ also have **certain** privacy, data protection, information security obligations arising from the practices in our industry or of companies similar to us. We are also bound by other contractual obligations related to privacy, data protection, and information security, and our efforts to comply with such obligations may not be successful. If we fall below such industry standard or cannot comply with such contractual obligations, our reputation and business may be harmed. We also publish privacy policies, marketing materials, **whitepapers** and other statements, such as compliance with certain certifications or self- regulatory principles, regarding privacy, data protection, **artificial intelligence** and information security. ~~If~~ **Regulators in the United States have scrutinized and are increasingly**

**scrutinizing these statements, and if** these policies, materials or statements are found to be deficient, lacking in transparency, deceptive, unfair, **misleading** or misrepresentative of our practices, we may be subject to investigation, enforcement actions by regulators, or other adverse consequences. Government Inquiries and Investigations We have in the past and may in the future receive inquiries or be subject to investigations by domestic and international government entities regarding, among other things, our privacy, data protection, and information security practices. The result of these proceedings could impact our brand reputation, subject us to monetary remedies and costs, interrupt or require us to change our business practices, divert resources and the attention of management from our business, or subject us to other remedies that adversely affect our business. We also face litigation regarding our privacy and security practices, including alleged data sharing with third parties, in various jurisdictions. See Part I, Item 3 " Legal Proceedings " for additional information. In June 2020, we received a grand jury subpoena from the Department of Justice' s U. S. Attorney' s Office for the EDNY, which requested information regarding our interactions with foreign governments and foreign political parties, including the Chinese government, as well as information regarding storage of and access to user data, the development and implementation of Zoom' s privacy policies, and the actions we took responding to law enforcement requests from the Chinese government. In July 2020, we received subpoenas from the Department of Justice' s U. S. Attorney' s Office for the NDCA and the SEC. Both subpoenas seek documents and information relating to various security, data protection, and privacy matters, including our encryption, and our statements relating thereto, as well as calculation of usage metrics and related public statements. In addition, the NDCA subpoena seeks information relating to any contacts between our employees and representatives of the Chinese government, and any attempted or successful influence by any foreign government in our policies, procedures, practices, and actions as they relate to users in the United States. We have since received additional subpoenas from EDNY and NDCA seeking related information. We are fully cooperating with all of these investigations and have **conducted** ~~been conducting~~ our own thorough internal investigation. These investigations are ongoing, and ~~we~~ **a negative outcome in any or all of these matters could cause us to incur substantial fines, penalties, or other financial exposure, as well as material reputational harm, a loss of customer and user confidence and business, additional expenses, and other harm to our business. As of the date hereof, in regard to the SEC matter, a tentative settlement of $ 18. 0 million is now outstanding and remains subject to SEC approval. We** do not know when ~~they~~ **these matters** will be completed **, including the SEC matter** , which facts we will ultimately discover as a result of the investigations, or what actions the government may or may not take ~~. We cannot predict the outcome of these investigations, and a negative outcome in any or all of these matters could cause us to incur substantial fines, penalties, or other financial exposure, as well as material reputational harm, a loss of customer and user confidence and business, additional expenses, and other harm to our business~~ . We were also the subject of an investigation by the FTC relating to our privacy and security representations and practices. We have reached a settlement agreement with the FTC, which the FTC voted to make final on January 19, 2021. We could fail or be perceived to fail to comply with the terms of the settlement with the FTC or any other orders or settlements relating to litigation or governmental investigations with respect to our privacy and security practices. Any failure or perceived failure to comply with such orders or settlements may increase the possibility of additional adverse consequences, including litigation, additional regulatory actions, injunctions, or monetary penalties, or require further changes to our business practices, significant management time, or the diversion of significant operational resources. Furthermore, the costs of compliance with, and other burdens imposed by, the laws, regulations, policies, and other obligations that are applicable to the businesses of our users may limit the adoption and use of, and reduce the overall demand for, our platform and services, which could have an adverse impact on our business. Consents Additionally, we rely on the administrators of our customers in the healthcare and education industries to obtain the necessary consents from users of our products and services and to ensure their account settings are configured correctly for their compliance under applicable laws and regulations, including HIPAA. Furthermore, if third parties we work with, such as vendors or developers, make misrepresentations, violate applicable laws and regulations, or our policies, such misrepresentations and violations may also put our users' content at risk and could in turn have an adverse effect on our business. Any significant change to applicable laws, regulations, or industry practices regarding the collection, use, retention, security, or disclosure of our users' content, or regarding the manner in which the express or implied consent of users for the collection, use, retention, or disclosure of such content is obtained, could increase our costs and require us to modify our services and features, possibly in a material manner, which we may be unable to complete and may limit our ability to store and process user data or provide or develop new services and features. Public Perception Increased usage of our services and additional awareness of Zoom and our brand has led to greater public scrutiny of, press related to, or a negative perception of our collection, use, storage, disclosure, and processing of personal information, and our privacy policies and practices. For example, users and customers, particularly those that are new to Zoom, may not have significant IT or security knowledge or have their own IT controls like those of a larger organization to configure our service in a manner that provides them with control over user settings. This has resulted in reports of users and customers experiencing meeting disruptions by malicious actors. Additional unfavorable publicity and scrutiny has led to increased governmental and regulatory scrutiny and litigation exposure, and could result in material reputational harm, a loss of customer and user confidence, additional expenses and other harm to our business. Failure to Comply with our Obligations Obligations related to privacy, data protection, information security, the use of AI, the provision of online services and other interactive platforms (and consumers' expectations regarding them) are quickly changing, becoming increasingly stringent, and creating uncertainty. Additionally, these obligations may be subject to differing applications and interpretations, which may be inconsistent or conflict among jurisdictions. Preparing for and complying with these obligations requires us to devote significant resources and **has and** may **continue to** necessitate changes to our services, information technologies, systems, and practices and to those of any third parties that process personal information on our behalf. We may at times fail (or be perceived to have failed) in our efforts to comply with our obligations relating to privacy, data protection, information security, the use of AI and the provision of online services and other interactive platforms. Moreover, despite our efforts, our personnel or third parties ~~on~~ **with** whom we ~~rely~~ **work** may fail to comply with such

obligations, which could negatively impact our business operations. If we or the third parties ~~on which~~ **with whom** we ~~rely~~ **work** fail, or are perceived to have failed, to address or comply with applicable privacy, data protection, and information security obligations, we could face significant consequences, including but not limited to: government enforcement actions (e. g., investigations, fines, penalties, audits, inspections, and similar); litigation (including class- action claims) and mass arbitration demands; additional reporting requirements and / or oversight; bans **or restrictions** on processing personal information; and orders to destroy or not use personal information. In particular, plaintiffs have become increasingly more active in bringing privacy- related claims against companies, including class claims and mass arbitration demands. Some of these claims allow for the recovery of statutory damages on a per violation basis, and, if viable, carry the potential for monumental statutory damages, depending on the volume of data and the number of violations. Any of these events could have a material adverse effect on our reputation, business, or financial condition, including but not limited to: loss of customers; inability to process personal information or to operate in certain jurisdictions; limited ability to develop or commercialize our products; expenditure of time and resources to defend any claim or inquiry; adverse publicity; or substantial changes to our business model or operations. Changes in government trade policies, including the imposition of tariffs and export restrictions, could limit our ability to sell our products to certain customers, which may materially adversely affect our sales and results of operations. The U. S. or foreign governments **have taken and** may **in the future** take administrative, legislative, or regulatory action **, including imposing tariffs,** that could materially interfere with our ability to sell products in certain countries ~~. For example, the Trump administration had threatened tougher trade terms with China and other countries, leading to the imposition, or announcement of future imposition, of substantially higher U. S. Section 301 tariffs on roughly $ 500 billion of imports from China. In response, China imposed and proposed new or higher tariffs on U. S. products~~ . The direct and indirect effects of tariffs and other restrictive trade policies are difficult to measure and are only one part of a larger U. S. / China economic and trade policy disagreement. The effects of tariffs are uncertain because of the dynamic nature of governmental action and responses. Sustained uncertainty about, or worsening of, current global economic conditions and further escalation of trade tensions between the United States and its trading partners, especially China, could result in a global economic slowdown and long- term changes to global trade, including retaliatory trade restrictions that restrict our ability to operate in China. We cannot predict what actions may ultimately be taken by the ~~Biden~~ **current** administration or future ~~administration~~ **administrations** with respect to tariffs or trade relations between the United States and China or other countries, what products may be subject to such actions, or what actions may be taken by the other countries in retaliation. Any further deterioration in the relations between the United States and China could exacerbate these actions and other governmental intervention. For example, the implementation of China' s national- security law in Hong Kong has created additional U. S.- China tensions and could potentially increase the risks associated with the business and operations of U. S.- based technology companies in China. Any alterations to our business strategy or operations made in order to adapt to or comply with any such changes would be time- consuming and expensive, and certain of our competitors may be better suited to withstand or react to these changes. Further, ~~in recent years,~~ the U. S. Government has expressed concerns with the security of information and communications technology and services (" ICTS ") sourced from providers in China, Russia, and other jurisdictions. In May 2019, ~~former President Trump issued~~ an executive order ~~that invoked~~ **was issued invoking** national emergency economic powers to implement a framework to regulate the acquisition or transfer of ICTS in transactions that imposed undue national security risks. The executive order is subject to implementation by the Secretary of Commerce and applies to contracts entered into prior to the effective date of the order. On March 22, 2021, the U. S. Department of Commerce issued an interim final rule allowing it to identify, review, and prohibit ICTS transactions that pose a national security risk, including transactions involving specified countries, such as China. Several aspects of this rule remain unclear including the scope of affected transactions and how the rule will be implemented and enforced in practice. In addition, the U. S. Commerce Department has implemented additional restrictions and may implement further restrictions that would affect conducting business with certain Chinese companies. Due to the uncertainty regarding the timing, content, and extent of any such changes in policy, we cannot assure you that we will successfully mitigate any negative impact. Depending upon their duration and implementation, these tariffs, the executive order and its implementation, and other regulatory actions could materially affect our business, including in the form of increased cost of revenue, decreased margins, increased pricing for customers, and reduced sales. We may be subject to additional liabilities on past sales for taxes, surcharges, and fees. We currently collect and remit applicable indirect taxes in jurisdictions where we, through our employees, have a presence and where we have determined, based on legal precedents in the jurisdiction, that sales of our platform are classified as taxable. State and local taxing authorities have differing rules and regulations that are subject to varying interpretations. This makes the applicability of sales tax to e- commerce businesses, such as ours, uncertain and complex. We believe that we are not otherwise subject to, or required to collect, additional taxes, fees, or surcharges imposed by state and local jurisdictions because we do not have a sufficient physical presence or " nexus " in the relevant taxing jurisdiction, or such taxes, fees, or surcharges do not apply to sales of our platform in the relevant taxing jurisdiction. There is uncertainty as to what constitutes sufficient nexus for sales made over the Internet and, after the U. S. Supreme Court' s ruling in South Dakota v. Wayfair, states may require an e- commerce business with no in- state property or personnel to collect and remit sales tax. Therefore, it is possible that we could face future audits or challenges of our positions by taxing authorities and that our liability for these taxes could exceed our estimates. The application of existing, new, or future laws, whether in the U. S. or internationally, could harm our business. We are subject to governmental export and import controls that could impair our ability to compete in international markets due to licensing requirements and subject us to liability if we are not in compliance with applicable laws. Our platform and associated products are subject to various restrictions under U. S. export control and sanctions laws and regulations, including the U. S. Department of Commerce' s Export Administration Regulations (" EAR ") and various economic and trade sanctions regulations administered by the U. S. Department of the Treasury' s Office of Foreign Assets Control (" OFAC "). The U. S. export control laws and U. S. economic sanctions laws include restrictions or prohibitions on the sale or supply of certain products and services

to U. S.- embargoed or U. S.- sanctioned countries, governments, persons, and entities, and also require authorization for the export of certain encryption items. In addition, various countries regulate the import of certain encryption technology, including through import permitting and licensing requirements and have enacted or could enact laws that could limit our ability to distribute our platform or could limit our customers' ability to implement our platform in those countries. Although we have taken precautions to prevent our platform and associated products from being accessed or used in violation of such laws, we have inadvertently allowed our platform and associated products to be accessed or used by some customers in potential violation of U. S. economic sanction laws. In addition, we have in the past inadvertently made and may inadvertently make our software products available to some customers in potential violation of the EAR. Therefore, as warranted, we may submit voluntary self-disclosures regarding compliance with U. S. sanctions and export control laws and regulations to OFAC and to the U. S. Department of Commerce' s Bureau of Industry and Security (" BIS "). For instance, in March 2022, we submitted a voluntary self- disclosure to BIS regarding our compliance with certain U. S. export control laws and regulations, which BIS closed out with a warning letter with no referral for criminal or administrative prosecution, and no imposition of monetary fines or penalties. If we are found to be in violation of U. S. economic sanctions or export control laws in the future, it could result in fines and penalties. We may also be adversely affected through other penalties, business disruption, reputational harm, loss of access to certain markets, or otherwise. While we are working to implement additional controls designed to prevent similar activity from occurring in the future, these controls may not be fully effective. Changes in our platform, or changes in export, sanctions, and import laws, may delay the introduction and sale of subscriptions to our platform in international markets; prevent our customers with international operations from using our platform; or, in some cases, prevent the access or use of our platform to and from certain countries, governments, persons, or entities altogether. Further, any change in export or import regulations, economic sanctions or related laws, 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 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 likely harm our business. We may be subject to, or respond to requests from law enforcement in connection with enforcement of, a variety of U. S. and international laws that could result in claims, increase the cost of operations or otherwise harm our business due to changes in the laws, changes in the interpretations of the laws, greater enforcement of the laws, or investigations into compliance with the laws. We may be subject to, or respond to requests from law enforcement that are legally valid, appropriately scoped, and sufficiently detailed in connection with enforcement of, various civil and criminal laws, including those covering copyright, indecent content, child protection, consumer protection, telecommunications services, taxation, and similar matters. It may be difficult, expensive, and disruptive for us to address law enforcement requests, subpoenas and other legal process, and laws in various jurisdictions may conflict and hamper our ability to satisfy or comply with such requests, subpoenas and other legal process. There have been instances where improper or illegal content has been shared on our platform without our knowledge. As a service provider and as a matter of policy, we do not monitor user meetings. However, to protect user safety and prevent conduct that is illegal, violent, or harmful to others, we enforce our terms of service through use of a mix of tools that suggest when such activity may be occurring on our platform. Our trust and safety team may take further action as appropriate, including suspension or termination of the participant' s account or referral to law enforcement. The laws in this area are currently in a state of flux and vary widely between jurisdictions. Accordingly, it may be possible that in the future we and our competitors may be subject to legal actions along with the users who shared such content. In addition, regardless of any legal liability we may face, our reputation could be harmed should there be an incident generating extensive negative publicity about the content shared on our platform. Such publicity would harm our business. Changes in law or policy could compel us or limit our ability to engage in content moderation, or otherwise limit the ability of users to engage in inappropriate or harmful behavior, and could expose us to liability. There have been various Congressional and executive efforts to eliminate or modify Section 230 of the Communications Act of 1934, enacted as part of the Communications Decency Act of 1996. Section 230 provides protection for providers of online service from liability for content produced by third parties and protects the right to engage in moderation of user content. ~~President Biden~~ **The current administration** and many ~~Members~~ **members** of Congress from both parties support the reform or repeal of Section 230, so the possibility of Congressional action remains. In addition, the FCC is considering a petition ~~, filed by the Trump Administration,~~ to adopt rules interpreting Section 230, which limits the liability of internet platforms for third- party content that is transmitted via those platforms and for good- faith moderation of offensive content. No date has been set for a vote on that proposal, and the FCC has not released any document describing the rules that would be proposed. ~~The Democratic members of the FCC have indicated that they are opposed to the petition and now control the agenda of the FCC.~~ There is no schedule for action by the FCC on the petition. If Congress revises or repeals Section 230 or the FCC adopts rules, we may no longer be afforded the same level of protection offered by Section 230. In addition, there are pending cases before the judiciary that may result in changes to the protections afforded to internet platforms, including a lawsuit ~~by former President Trump~~ that, if successful, would greatly limit the scope of Section 230. The U. S. Supreme Court recently declined to limit the applicability of Section 230 in certain circumstances, but future cases may not yield the same results **and a recent decision by the U. S. Court of Appeals for the Third Circuit would limit the applicability of Section 230 to curated content** . These various efforts to limit the protections provided by Section 230 would increase the risks faced by internet- based businesses, like Zoom, that rely on third- party content. Even if claims asserted against us do not result in liability, we may incur substantial costs in investigating and defending such claims. If we are found liable for our customers' or other users' activities, we could be required to pay fines or penalties, redesign business methods, or otherwise expend resources to remedy any damages caused by such actions and to avoid future liability. Legislation has been adopted in Florida and Texas that is intended to reduce or eliminate the power of businesses operating on the Internet to moderate user- generated content, implicitly eliminating the federal protections granted under Section 230. Similar legislation has been introduced in other

states ~~in 2022, including a bill that has passed the Georgia State Senate and is pending before the Georgia House~~ . Implementation of the Florida and Texas statutes has been stayed by various federal courts, including the U. S. Supreme Court. On August 18, **2022,** the parties in the Florida case requested, and were granted, a stay of the appeals court mandate pending Supreme Court review. On September 16, 2022, the U. S. Court of Appeals for the Fifth Circuit issued a decision upholding the Texas law. On September 30, the parties in that case filed an unopposed motion to stay the Fifth Circuit decision pending Supreme Court review, and the Fifth Circuit granted that request on October 13, 2022. On September 29, 2023, the Supreme Court announced that **it** would review both the Florida and Texas decisions **, and on July 1, 2024, the Court issued a decision returning both cases to the trial courts for additional analysis** . ~~A~~ **The district court in Texas, on August 29, 2024, issued a decision staying some portions of the Texas law and allowing others to go into effect, relying on analysis under both Section 230 and the First Amendment, and on November 18, 2024, the Fifth Circuit issued an order setting parameters for the district court' s consideration of the issues raised by the** Supreme Court ~~decision is expected during the first half of 2024~~ . **The district court in** Florida ~~recently~~ **set a trial date in its case for June 2025. Florida** amended its statute in an effort to address issues that led the court to issue the stay. It is likely that any other such state legislation also would be challenged under the First Amendment to the U. S. Constitution and on the ground that it is preempted by **Section 230. In addition, on August 27, 2024, the U. S. Court of Appeals for the Third Circuit issued a decision limiting the protections afforded by Section 230 in cases where a social media company curates user feeds to the extent that the feed becomes the speech of the company, reversing a trial court decision that immunized the company under** Section 230. We cannot predict whether any such state legislation will be adopted, enforced, modified, overturned, or vacated. Furthermore, new laws and regulations have been enacted or are being considered that impose extensive obligations regarding online safety and the operation of online services or platforms, such as the OSA and DSA, which may increase our compliance costs, require changes to our processes, operations, and business practices. For example, these new laws and regulations may seek to regulate the sharing of user - generated content and require us to identify, mitigate, and manage the risks of harm to users from illegal or harmful content. Violating these obligations could carry significant consequences. For example, violating the DSA can result in fines of up to 6 % of total annual worldwide revenue and violating the OSA can result in audits, inspections, and fines of up to £ 18 million or 10 % of worldwide revenue, whichever is higher. Zoom Phone is subject to U. S. federal and international regulation, and other products we may introduce in the future may also be subject to U. S. federal, state, or international laws, rules, and regulations. Any failure to comply with such laws, rules, and regulations could harm our business and expose us to liability. Federal Regulation Zoom Phone is provided through our wholly owned subsidiary, Zoom Voice Communications, Inc., which is regulated by the FCC as an interconnected voice over internet protocol (“ VoIP ”) service provider. As a result, Zoom Phone is subject to existing or potential FCC regulations, including, but not limited to, regulations relating to privacy, disability access, porting of numbers, federal Universal Service Fund (“ USF ”), contributions and other regulatory assessments, emergency calling / Enhanced 911 (“ E- 911 ”), access charges for long distance services, and law enforcement access. **The Supreme Court currently is considering a challenge to the USF contribution rules that could affect how such contributions are collected from services providers like us.** Congress or the FCC may expand the scope of Zoom Phone’ s regulatory obligations at any time. In addition, FCC classification of Zoom Phone as a common carrier or telecommunications service could result in additional federal and state regulatory obligations. If we do not comply with any current or future state regulations that apply to our business, we could be subject to substantial fines and penalties, we may have to restructure our product offerings, exit certain markets, or raise the price of our products, any of which could ultimately harm our business and results of operations. Any enforcement action by the FCC, which may be a public process, would hurt our reputation in the industry, possibly impair our ability to sell Zoom Phone to our customers and harm our business. As described above, the FCC ~~could~~ **has** ~~reinstate~~ **reinstated** its prior network neutrality regulations ~~or adopt new regulations~~ **, but the FCC order was reversed by the Sixth Circuit Court of Appeals** . See Part 1A. Failures in internet infrastructure or interference with broadband access could cause current or potential users to believe that our systems are unreliable, possibly leading our customers to switch to our competitors, or to cancel their subscriptions to our platform. Changes in FCC regulation of the internet and internet- based services also could impose new regulatory obligations on our other services. Such action could result in extension of common carrier regulation to internet- based communications services like the ones we offer. The imposition of common carrier regulation would increase our costs, and we could be required to modify our service offerings to comply with regulatory requirements. The failure to comply with such regulation could result in substantial fines and penalties and other sanctions. On December 13, 2023, the FCC adopted revised rules on reporting of breaches of private customer information, known as CPNI. The revised rules could broaden the types of CPNI breaches that must be reported, but also could limit the number of reports that must be filed by adopting a minimum threshold for the number of customers affected and not requiring reporting in certain circumstances when customers are not harmed. The rules also require that breach reports be provided directly to the FCC, which could increase the risk of enforcement action, including fines and behavioral remedies. These rules are not yet in effect **and have been challenged in federal court. We cannot predict the impact of the new rules on our operations or business or whether they will be overturned in court** . The FCC has adopted rules that prohibit Chinese companies that are deemed to be a national security risk by other federal agencies from obtaining new authorizations and placed on a list known as the Covered List to sell telecommunications equipment in the U. S. and is considering proposed rules that would ban those companies from selling previously- authorized equipment or could prohibit **the** use of their equipment in the U. S. Zoom does not currently have any equipment from the companies subject to the ban in its network, but if other companies are added to the Covered List and the FCC adopts rules that ban sales or use of equipment from such companies, we could be required to find new sources for similar equipment or replace existing equipment entirely. State Regulation State telecommunications regulation of Zoom Phone is generally preempted by the FCC. However, states are allowed to assess state USF contributions, E- 911 fees, and other surcharges. A number of states require us to contribute to state USF and pay E- 911 and other assessments and surcharges, while

others are actively considering extending their programs to include the products we offer. The California Public Utilities Commission **has adopted** ~~is now taking the position that it can~~ **an order** ~~require~~ **requiring** VoIP providers like Zoom Phone to obtain authority to operate in that state. We generally pass USF, E- 911 fees, and other surcharges through to our customers where we are permitted to do so, which may result in our products becoming more expensive. We expect that state public utility commissions will continue their attempts to apply state telecommunications regulations to services like Zoom Phone. If we do not comply with any current or future state regulations that apply to our business, we could be subject to substantial fines and penalties, and we may have to restructure our product offerings, exit certain markets, or raise the price of our products, any of which could harm our business. Certain states have adopted or are adopting or considering legislation or executive actions that would regulate the conduct of broadband providers. California' s state- specific network neutrality law has taken effect and Vermont' s law took effect, but a challenge to that law remains pending. **The FCC' s April 25 order permits it to preempt any state- level network neutrality requirements that go beyond the requirements adopted in that order, but specifically held that the California law would not be preempted. The FCC order was stayed on August 1, 2024, pending resolution of an appeal. For additional information on this order, see the risk factor titled " Failures in internet infrastructure or interference with broadband access could cause current or potential users to believe that our systems are unreliable, possibly leading our customers to switch to our competitors, or to cancel their subscriptions to our platform. "** We cannot predict whether other state initiatives will be enforced, modified, overturned, or vacated. International Regulation As we expand internationally, we may be subject to telecommunications, consumer protection, privacy, data protection, and other laws and regulations in the foreign countries where we offer our products. If we do not comply with any current or future international regulations that apply to our business, we could be subject to substantial fines and penalties, we may have to restructure our product offerings, exit certain markets, or raise the price of our products, any of which could harm our business. Risks Related to Our Intellectual Property We are currently, and may be in the future, party to intellectual property rights claims and other litigation matters, which, if resolved adversely, could harm our business. We protect our intellectual property through patents, copyrights, trademarks, domain names, and trade secrets and, from time to time, are subject to litigation based on allegations of infringement, misappropriation, or other violations of intellectual property or other **proprietary** rights **of others** . Some companies, including some of our competitors, own large numbers of patents, **as well as valuable** copyrights ~~,~~ and trademarks, which they may use to assert claims against us. As we face increasing competition and gain an increasingly high profile, the possibility of intellectual property rights claims, commercial claims, and other assertions against us grows. We have in the past been, are currently, and may from time to time in the future become, a party to litigation and disputes related to our **use of** intellectual property, our business practices, and our platform. While we intend to defend these lawsuits vigorously and believe that we have valid defenses to these claims, litigation can be costly and time consuming, divert the attention of our management and key personnel from our business operations and dissuade potential customers from subscribing to our services, which would harm our business. Furthermore, with respect to these lawsuits, there can be no assurances that favorable outcomes will be obtained. We may need to settle litigation and disputes on terms that are unfavorable to us, or we may be subject to an unfavorable judgment that may not be reversible upon appeal. The terms of any settlement or judgment may require us to cease some or all of our operations or pay substantial amounts to the other party. In addition, our agreements with certain larger customers include certain provisions for indemnifying them against liabilities if our services infringe a third party' s intellectual property rights, which could require us to make payments to our customers. During the course of any litigation or dispute, we may make announcements regarding the results of hearings and motions and other interim developments. If securities analysts and investors regard these announcements as negative, the market price of our Class A common stock may decline. With respect to any intellectual property rights claim, we may have to seek a license to continue practices found to be in violation of third- party rights, which may not be available on reasonable terms and may significantly increase our operating expenses. A license to continue such practices may not be available to us at all, and we may be required to develop alternative non- infringing technology or practices or discontinue the practices. The development of alternative, non- infringing technology or practices could require significant effort and expense. Our business could be harmed as a result. Our failure to protect our intellectual property rights and proprietary information could diminish our brand and other intangible assets. We primarily rely and expect to continue to rely on a combination of patent, **trademark** ~~patent licenses, trade secret~~ and domain name protection, trademark and copyright laws, as well as confidentiality and license agreements with our employees, consultants, and third parties, to protect our intellectual property and proprietary rights. We make business decisions about when to seek patent protection for a particular technology and when to rely upon copyright or trade secret protection, and the approach we select may ultimately prove to be inadequate. Even in cases where we seek patent protection, there is no assurance that the resulting patents will effectively protect every significant feature of our products. In addition, we believe that the protection of our trademark rights is an important factor in product recognition, protecting our brand and maintaining goodwill. If we do not adequately protect our rights in our trademarks from infringement and unauthorized use, any goodwill that we have developed in those trademarks could be lost **, diminished** or impaired, which could harm our brand and our business. Third parties may knowingly or unknowingly infringe our **intellectual property or** proprietary rights; third parties may challenge our **intellectual property or** proprietary ~~right~~ **rights** ; our pending and future patent, trademark, and copyright applications may not be approved; and we may not be able to prevent infringement without incurring substantial expense. We have also devoted substantial resources to the development of our proprietary technologies and related processes. In order to protect our proprietary technologies and processes, we rely in part on trade secret laws and confidentiality agreements with our employees, consultants, and third parties. These agreements may not effectively prevent disclosure of confidential information and may not provide an adequate remedy in the event of unauthorized disclosure of confidential information. In addition, others may **develop similar technologies or processes, or** independently discover our trade secrets, in which case we would not be able to assert **our** trade secret rights ~~, or develop similar technologies and processes~~ . Further, the laws of certain foreign countries do not provide the same level of

**intellectual property** protection of corporate proprietary information and assets such as ~~intellectual property~~ **rights to patents, copyrights** , trademarks, trade secrets, know- how, and records, as the laws of the United States. For instance, the legal systems of certain countries, particularly certain developing countries, do not favor the enforcement of patents and other intellectual property protection. As a result, we may encounter significant problems in protecting and defending our intellectual property or proprietary rights abroad. Additionally, we may also be exposed to material risks of theft or unauthorized reverse engineering of our proprietary information and other intellectual property, including technical data, manufacturing processes, data sets, or other sensitive information. Our efforts to enforce our intellectual property rights in such foreign countries may be inadequate to obtain a significant commercial advantage from the intellectual property that we develop, which could have a material adverse effect on our business, financial condition, and results of operations. Costly and time- consuming litigation could be necessary to enforce and determine the scope of our proprietary rights. If the protection of our proprietary rights is inadequate to prevent use or appropriation by third parties, the value of our platform, brand, and other intangible assets may be diminished, and competitors may be able to more effectively replicate our platform and its features. Any of these events would harm our business. Our use of third- party open source software could negatively affect our ability to offer and sell subscriptions to our platform and subject us to possible litigation. We have incorporated, and may in the future incorporate, third- party open source software **(including our open source AI models)** in our technologies. Open source software is generally licensed by its authors or other third parties under open source licenses. From time to time, companies that use third- party open source software have faced claims challenging the use of such open source software and requesting compliance with the open source software license terms. Accordingly, we may be subject to suits by parties claiming ownership of what we believe to be open source software or claiming non- compliance with the applicable open source licensing terms. Some open source software licenses require end- users who use, distribute or make available across a network software and services that include open source software to offer aspects of the technology that incorporates the open source software for no cost. We may also be required to make publicly available source code (which in some circumstances could include valuable proprietary code) for modifications or derivative works we create based upon incorporating or using the open source software and / or to license such modifications or derivative works under the terms of the particular open source license. Additionally, if a third- party software provider has incorporated open source software into software that we license from such provider, we could be required to disclose our source code that incorporates or is a modification of such licensed software. While we use tools designed to help us monitor and comply with the licenses of third- party open source software and protect our valuable proprietary source code, we may inadvertently use third- party open source software in a manner that exposes us to claims of non- compliance with the terms of their licenses, including claims of intellectual property rights infringement or for breach of contract. Furthermore, there exists today an increasing number of types of open source software licenses, almost none of which have been tested in courts of law to provide guidance of their proper legal interpretations. If we were to receive a claim of non- compliance with the terms of any of these open source licenses, we could be required to publicly release certain portions of our proprietary source code. We could also be required to expend substantial time and resources to re- engineer some of our software. Any of the foregoing could disrupt and harm our business. **Furthermore, with respect to our use of third party open source AI models, some licenses to third party open source AI models contain additional use restrictions pertaining to research- only limitations or, in some cases, vague notions of responsible uses for the AI models, which may not in all instances comport with our business practices.** In addition, the use of third- party open source software typically exposes us to greater risks than the use of third- party commercial software because open source licensors generally do not provide warranties or controls on the functionality or origin of the software. Use of open source software may also present additional security risks because the public availability of such software may make it easier for hackers and other third parties to determine how to compromise our platform. Any of the foregoing could harm our business and could help our competitors develop products and services that are similar to or better than ours. Risks Related to Ownership of Our Class A Common Stock The trading price of our Class A common stock may be volatile, and you could lose all or part of your investment. The trading price of our Class A common stock has been and will likely continue to be volatile and could be subject to fluctuations in response to various factors, some of which are beyond our control. 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 trading price of our Class A common stock include the following: • price and volume fluctuations in the overall stock market from time to time; • volatility in the trading prices and trading volumes of technology stocks; • changes in operating performance and stock market valuations of other technology companies generally, or those in our industry in particular; • sales of shares of our Class A common stock by us or our stockholders; • failure of securities analysts to maintain coverage of us, changes in financial estimates by securities analysts who follow our company, or our failure to meet these estimates or the expectations of investors; • the financial projections we may provide to the public, any changes in those projections, or our failure to meet those projections; • announcements by us or our competitors of new products, features, or services; • the public' s reaction to our press releases, other public announcements, and filings with the SEC; • rumors and market speculation involving us or other companies in our industry; • actual or anticipated changes in our results of operations or fluctuations in our results of operations; • actual or anticipated developments in our business, our competitors' businesses, or the competitive landscape generally; • litigation 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 or other proprietary rights; • announced or completed acquisitions of businesses, products, services, or technologies by us or our competitors; • new laws or regulations or new interpretations of existing laws or regulations applicable to our business; • changes in accounting standards, policies, guidelines, interpretations, or principles; • any significant change in our management; and • general political, social, economic and market conditions, in both domestic and our foreign markets, including effects of increased interest rates and inflationary pressures. In addition, in the past, following periods of volatility in the overall market and in the market price of a particular company' s securities, securities class action litigation has often been instituted against these companies. For

example, in April 2020, June 2020, July 2020 and October 2021, we and certain of our officers and directors were sued in putative class action lawsuits and purported shareholder derivative lawsuits alleging violations of the federal securities laws for allegedly making materially false and misleading statements about our data privacy and security measures. Securities litigation against us could result in substantial costs and divert our management' s time and attention from other business concerns, which could harm our business. We may be the target of additional litigation of this type in the future as well. The dual class structure of our common stock as contained in our amended and restated certificate of incorporation has the effect of concentrating voting control with those stockholders who held our stock prior to our IPO, including our executive officers, employees, and directors and their affiliates, limiting your ability to influence corporate matters. Our Class B common stock has 10 votes per share and our Class A common stock has one vote per share. As of January 31, ~~2024~~ **2025**, the holders of our outstanding Class B common stock held ~~64~~ **61**. ~~1~~ **8** % of the voting power of our outstanding capital stock, with our directors, executive officers and 5 % stockholders and their respective affiliates holding ~~56~~ **57**. ~~8~~ **0** % of such voting power in the aggregate. As of January 31, ~~2024~~ **2025**, our founder, President and Chief Executive Officer, Eric S. Yuan, together with his affiliates, held approximately 7. ~~4~~ **2** % of our outstanding capital stock but controlled approximately 31. ~~0~~ **8** % of the voting power of our outstanding capital stock. Therefore, these holders have significant influence over our management and affairs and over all matters requiring stockholder approval, including election of directors and significant corporate transactions, such as a merger or other sale of Zoom or our assets, for the foreseeable future. Each share of Class B common stock will be automatically converted into one share of Class A common stock upon the earliest of (i) the date that is six months following the death or incapacity of Mr. Yuan, (ii) the date that is six months following the date that Mr. Yuan is no longer providing services to us or his employment is terminated for cause, (iii) the date specified by the holders of a majority of the then outstanding shares of Class B common stock, voting as a separate class, and (iv) the 15- year anniversary of the closing of our IPO. In addition, the holders of Class B common stock collectively will continue to be able to control all matters submitted to our stockholders for approval even if their stock holdings represent less than a majority of the outstanding shares of our common stock. This concentrated control will limit your ability to influence corporate matters for the foreseeable future, and, as a result, the market price of our Class A common stock could be adversely affected. Future transfers by holders of Class B common stock will generally result in those shares converting to Class A common stock, which will have the effect, over time, of increasing the relative voting power of those holders of Class B common stock who retain their shares in the long term. If, for example, Mr. Yuan retains a significant portion of his holdings of Class B common stock for an extended period of time, he could, in the future, control a majority of the combined voting power of our Class A and Class B common stock. As a board member, Mr. Yuan owes a fiduciary duty to our stockholders and must act in good faith in a manner he reasonably believes to be in the best interests of our stockholders. As a stockholder, even a controlling stockholder, Mr. Yuan is entitled to vote his shares in his own interests, which may not always be in the interests of our stockholders generally. Future sales and issuances of our capital stock or rights to purchase capital stock could result in additional dilution of the percentage ownership of our stockholders and could cause our stock price to decline. Future sales and issuances of our capital stock or rights to purchase our capital stock could result in substantial dilution to our existing stockholders. We may sell Class A common stock, convertible securities, and other equity securities in one or more transactions at prices and in a manner as we may determine from time to time. If we sell any such securities in subsequent transactions, investors may be materially diluted. New investors in such subsequent transactions could gain rights, preferences, and privileges senior to those of holders of our Class A common stock. Substantial future sales of shares of our Class A common stock and Class B common stock 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 and Class B common stock (after automatically converting to Class A common stock) in the public market, or the perception that these sales might occur, could depress the market price of our Class A common stock. In addition, certain of our stockholders have registration rights that would require us to register shares owned by them for public sale in the United States. We have also filed a registration statement to register shares reserved for future issuance under our equity compensation plans. As a result, subject to the satisfaction of applicable exercise periods and applicable volume and restrictions that apply to affiliates, the shares issued upon exercise of outstanding stock options or upon settlement of outstanding restricted stock unit (" RSU ") awards are available for immediate resale in the United States in the open market. Sales of our shares could also impair our ability to raise capital through the sale of additional equity securities in the future and at a price we deem appropriate. These sales could also cause the trading price of our Class A common stock to fall and make it more difficult for you to sell shares of our Class A common stock. Provisions in our corporate charter documents and under Delaware law may prevent or frustrate attempts by our stockholders to change our management or hinder efforts to acquire a controlling interest in us, and the market price of our Class A common stock may be lower as a result. There are provisions in our certificate of incorporation and bylaws that may make it difficult for a third party to acquire, or attempt to acquire, control of Zoom, even if a change in control was considered favorable by our stockholders. Our charter documents also contain other provisions that could have an anti- takeover effect, such as: • establishing a classified board of directors so that not all members of our board of directors are elected at one time; • permitting the board of directors to establish the number of directors and fill any vacancies and newly created directorships; • providing that directors may only be removed for cause; • prohibiting cumulative voting for directors; • requiring super- majority voting to amend some provisions in our certificate of incorporation and bylaws; • authorizing the issuance of " blank check " preferred stock that our board of directors could use to implement a stockholder rights plan; • eliminating the ability of stockholders to call special meetings of stockholders; • prohibiting stockholder action by written consent, which requires all stockholder actions to be taken at a meeting of our stockholders; and • our dual- class common stock structure as described above. Moreover, because we are incorporated in Delaware, we are governed by the provisions of Section 203 of the Delaware General Corporation Law, which prohibit a person who owns 15 % or more of our outstanding voting stock from merging or combining with us for a period of three years after the date of the transaction in which the person acquired in excess of 15 % of our outstanding voting stock, unless the merger or

combination is approved in a prescribed manner. Any provision in our certificate of incorporation or our bylaws or Delaware law that has the effect of delaying or deterring a change in control could limit the opportunity for our stockholders to receive a premium for their shares of our Class A common stock and could also affect the price that some investors are willing to pay for our Class A common stock. Our amended and restated certificate of incorporation designates the Court of Chancery of the State of Delaware and the federal district courts of the United States of America as the exclusive forums for certain disputes between us and our stockholders, which could limit our stockholders' ability to choose the judicial forum for disputes with us or our directors, officers, or employees. Our amended and restated certificate of incorporation provides that, unless we consent in writing to the selection of an alternative forum, the sole and exclusive forum for the following types of actions or proceedings under Delaware statutory or common law: (i) any derivative action or proceeding brought on our behalf; (ii) any action asserting a claim of breach of a fiduciary duty owed by any of our directors, officers, or other employees to us or our stockholders; (iii) any action arising pursuant to any provision of the Delaware General Corporation Law, or the certificate of incorporation or the amended and restated bylaws; or (iv) any other action asserting a claim that is governed by the internal affairs doctrine shall be the Court of Chancery of the State of Delaware (or, if the Court of Chancery does not have jurisdiction, the federal district court for the District of Delaware), in all cases subject to the court having jurisdiction over indispensable parties named as defendants. This provision would not apply to suits brought to enforce a duty or liability created by the Exchange Act. Furthermore, Section 22 of the Securities Act creates concurrent jurisdiction for federal and state courts over all such Securities Act actions. Accordingly, both state and federal courts have jurisdiction to entertain such claims. To prevent having to litigate claims in multiple jurisdictions and the threat of inconsistent or contrary rulings by different courts, among other considerations, our amended and restated certificate of incorporation provides that the federal district courts of the United States of America will be the exclusive forum for resolving any complaint asserting a cause of action arising under the Securities Act. While the Delaware courts have determined that such choice of forum provisions are facially valid, a stockholder may nevertheless seek to bring a claim in a venue other than those designated in the exclusive forum provisions. In such instance, we would expect to vigorously assert the validity and enforceability of the exclusive forum provisions of our amended and restated certificate of incorporation. This may require significant additional costs associated with resolving such action in other jurisdictions and there can be no assurance that the provisions will be enforced by a court in those other jurisdictions. Any person or entity purchasing or otherwise acquiring any interest in any of our securities shall be deemed to have notice of and consented to these provisions. These exclusive- forum provisions may limit a stockholder' s ability to bring a claim in a judicial forum of its choosing for disputes with us or our directors, officers, or other employees, which may discourage lawsuits against us and our directors, officers and other employees. If a court were to find either exclusive- forum provision in our amended and restated certificate of incorporation to be inapplicable or unenforceable in an action, we may incur further significant additional costs associated with resolving the dispute in other jurisdictions, all of which could harm our results of operations. We do not intend to pay dividends for the foreseeable future. We have never declared nor paid cash dividends on our capital stock. We currently intend to retain any future earnings to finance the operation and expansion of our business, and we do not expect to declare or pay any dividends in the foreseeable future. As a result, stockholders must rely on sales of their Class A common stock after price appreciation as the only way to realize any future returns on their investment. General Risk Factors Estimates of our market opportunity and forecasts of market growth may prove to be inaccurate, and even if the market in which we compete achieves the forecasted growth, our business could fail to grow at similar rates, if at all. Market opportunity estimates and growth forecasts for the markets in which we compete, including those we have generated ourselves, are subject to significant uncertainty and are based on assumptions and estimates that may not prove to be accurate. Not every organization covered by our market opportunity estimates will necessarily buy video communications and collaboration platforms, and some or many of those organizations may choose to continue using legacy communication methods or point solutions offered by our competitors. It is impossible to build every product feature that every customer or user wants, and our competitors may develop and offer features that our platform does not provide. The variables that go into the calculation of our market opportunity are subject to change over time, and there is no guarantee that any particular number or percentage of the organizations covered by our market opportunity estimates will purchase our solutions at all or generate any particular level of revenue for us. Even if the markets in which we compete meet the size estimates and growth forecasts, our business could fail to grow for a variety of reasons outside of our control, including competition in our industry. If any of these risks materializes, it could harm our business and prospects. Our business could be disrupted by catastrophic events. Occurrence of any catastrophic event, including earthquake, fire, flood, tsunami or other weather event, power loss, telecommunications failure, software or hardware malfunctions, cyber- attack, war, terrorist attack, disease, or health epidemics, could result in lengthy interruptions in our service. In particular, our U. S. headquarters and some of the data centers we utilize are located in the San Francisco Bay Area, a region known for seismic activity, and our insurance coverage may not compensate us for losses that may occur in the event of an earthquake or other significant natural disaster. In addition, acts of terrorism could cause disruptions to the internet or the economy as a whole. Even with our disaster recovery arrangements, our service could be interrupted. Moreover, if our systems were to fail or be negatively impacted as a result of a natural disaster or other event, our ability to deliver products to our users would be impaired, or we could lose critical data. If we are unable to develop adequate plans to ensure that our business functions continue to operate during and after a disaster and to execute successfully on those plans in the event of a disaster or emergency, our business would be harmed. We also face risks related to health epidemics. An outbreak of a contagious disease, and other adverse health developments could have an adverse effect on global economic conditions and on our business. The effects could include business and service disruptions, such as the temporary closure of our facilities, restrictions on our employees' ability to travel to support our facilities and services, and difficulties in hiring new employees. We are subject to risks associated with our strategic investments, including partial or complete loss of invested capital. Significant changes in the fair value of our investment portfolio could negatively impact our financial results. We have strategic investments in publicly traded and privately held companies. The financial success of our

investments in any privately held company is typically dependent on a liquidity event, such as a public offering, acquisition or other favorable market event reflecting appreciation to the cost of our initial investment. In addition, valuations of privately held companies are inherently complex due to the lack of readily available market data. Likewise, the financial success of our investment in any publicly held company is typically dependent upon an exit in favorable market conditions, and to a lesser extent on liquidity events. The capital markets for public offerings and acquisitions are currently depressed and the likelihood of successful liquidity events for the companies we have invested in could significantly worsen. In addition, valuations of privately held companies are inherently complex due to the lack of readily available market data. We record all fair value adjustments of our publicly traded and privately held non- marketable securities through the consolidated statement of operations. As a result, we may experience additional volatility to our statements of operations due to changes in market prices of our investments in publicly held securities and the valuation and timing of observable price changes or impairments of our investments in privately held securities. Our ability to mitigate this volatility in any given period may be impacted by our contractual obligations to hold securities for a set period of time. All of our investments are subject to a risk of a partial or total loss of investment capital. Changes in the fair value or partial or total loss of investment capital of these individual companies could be material to our financial statements and negatively impact our business and financial results. Our reported results of operations may be adversely affected by changes in accounting principles generally accepted in the United States. Generally accepted accounting principles in the United States are subject to interpretation by the FASB, the SEC, and various bodies formed to promulgate and interpret appropriate accounting principles. A change in these principles or interpretations could have a significant effect on our reported results of operations and may even affect the reporting of transactions completed before the announcement or effectiveness of a change. It is also difficult to predict the impact of future changes to accounting principles or our accounting policies, any of which could harm our business. We may need additional capital, and we cannot be certain that additional financing will be available on favorable terms, or at all. Historically, we have funded our operations and capital expenditures primarily through equity issuances and cash generated from our operations. Although we currently anticipate that our existing cash and cash equivalents and cash flow from operations will be sufficient to meet our cash needs for the foreseeable future, we may require additional financing. We evaluate financing opportunities from time to time, and our ability to obtain financing will depend, among other things, on our development efforts, business plans, operating performance, and condition of the capital markets at the time we seek financing. We cannot assure you that additional financing will be available to us on favorable terms when required, or at all, particularly during times of market volatility and general economic instability. The need for additional liquidity may also be affected by the federal government' s potential failure to raise the debt ceiling or correct a prolonged banking or financial crisis. If we raise additional funds through the issuance of equity or equity- linked or debt securities, those securities may have rights, preferences, or privileges senior to the rights of our Class A common stock, and our stockholders may experience dilution. If we fail to maintain an effective system of disclosure controls and internal control over financial reporting, our ability to produce timely and accurate consolidated financial statements or comply with applicable regulations could be impaired. We are subject to the reporting requirements of the Exchange Act, the Sarbanes- Oxley Act of 2002 (the " Sarbanes- Oxley Act ") and the rules and regulations of the applicable listing standards of The Nasdaq Stock Market. 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 and other procedures that are designed to ensure that information required to be disclosed by us 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 that information required to be disclosed in reports under the Exchange Act is accumulated and communicated to our principal executive and financial officers. We are also continuing to improve our internal control over financial reporting. In order to maintain and improve the effectiveness of our disclosure controls and procedures and internal control over financial reporting, we have expended, and anticipate that we will continue to expend, significant resources in our accounting, legal and IT organizations. Our current controls and any new controls that we develop may become inadequate because of changes in conditions in our business. In addition, changes in accounting principles or interpretations could also challenge our internal controls and require that we establish new business processes, systems, and controls to accommodate such changes. We have limited experience with implementing the systems and controls that will be necessary to operate as a public company, as well as adopting changes in accounting principles or interpretations mandated by the relevant regulatory bodies. Additionally, if these new systems, controls, or standards and the associated process changes do not give rise to the benefits that we expect or do not operate as intended, it could adversely affect our financial reporting systems and processes, our ability to produce timely and accurate financial reports, or the effectiveness of internal control over financial reporting. Moreover, our business may be harmed if we experience problems with any new systems and controls that result in delays in their implementation or increased costs to correct any post- implementation issues that may arise. Further, weaknesses in our disclosure controls and internal control over financial reporting 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 business or cause us to fail to meet our reporting obligations and may result in a restatement of our consolidated financial statements for prior periods. Any failure to implement and maintain effective internal control over financial reporting also 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 will eventually be required to include in our periodic reports that will be filed with the SEC. Recently, the SEC has alleged violations of internal controls at other public companies, even in the absence of an underlying accounting or disclosure violation, which significantly increases the enforcement risk faced by us and other public companies for any weaknesses in disclosure controls and internal control over financial reporting. 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 trading price of our Class A common stock. In addition, if we are unable to continue to meet these requirements, we may not be able to remain listed on The Nasdaq Stock Market. We are required to provide an annual management report on the effectiveness of our internal control over financial reporting. Our independent registered public accounting firm is required to formally attest to the effectiveness of our internal control over financial reporting. Our independent registered public accounting firm may issue a report that is adverse in the event it is not satisfied with the level at which our internal control over financial reporting is documented, designed, or operating. Any failure to maintain effective disclosure controls and internal control over financial reporting could harm our business and could cause a decline in the trading price of our Class A common stock. Our Class A common stock market price and trading volume could decline if securities or industry analysts do not publish research or publish inaccurate or unfavorable research about our business. The trading market for our Class A common stock depends in part on the research and reports that securities or industry analysts publish about us or our business. The analysts' estimates are based upon their own opinions and are often different from our estimates or expectations. If one or more of the analysts who cover us downgrade our Class A common stock or publish inaccurate or unfavorable research about our business, the price of our securities would likely decline. If one or more securities analysts cease coverage of us or fail to publish reports on us regularly, demand for our securities could decrease, which might cause the price and trading volume of our Class A common stock to decline. We incur costs and demands upon management as a result of complying with the laws and regulations affecting public companies in the United States, which may harm our business. As a public company listed in the United States, we incur significant additional legal, accounting, and other expenses. In addition, changing laws, regulations, and standards relating to corporate governance and public disclosure, including regulations implemented by the SEC and The Nasdaq Stock Market, may increase legal and financial compliance costs and make some activities more time consuming. These laws, regulations, and standards are subject to varying interpretations, and as a result, their application in practice may evolve over time as new guidance is provided by regulatory and governing bodies. We intend 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, notwithstanding our efforts, we fail to comply with new laws, regulations, and standards, regulatory authorities may initiate legal proceedings against us and our business may be harmed. Failure to comply with these rules might also make it more difficult for us to obtain certain types of insurance, including director and officer liability insurance, and we might be forced to accept reduced policy limits and coverage or incur substantially higher costs to obtain the same or similar coverage. The impact of these events would also make it more difficult for us to attract and retain qualified persons to serve on our board of directors, on committees of our board of directors, or as members of senior management. Regulators', investors' and other stakeholders' 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 regulators, investors, customers and other stakeholders concerning environmental, social and governance matters ~~(" ESG ")~~. **To** ~~Regulators are driving legislation to bring consistency and transparency to ESG disclosures. Some investors may use these ESG performance factors to guide their investment strategies and, in some cases, may choose not to invest in us if they~~ **the extent we** ~~believe our policies and actions relating to ESG are~~ **share information about** ~~inadequate. We may face reputational damage in the event that we do not meet the ESG standards set by various constituencies. Our voluntary ESG and climate disclosures, as well as our reporting under related disclosure regulations, or~~ **our** ~~a failure to meet evolving stakeholder expectations for ESG reporting and~~ practices ~~, may potentially harm our reputation and customer relationships or expose us to liability. Due to new regulatory standards and market standards, certain new or existing customers may impose stricter ESG guidelines or contractual language for, and may scrutinize relationships more closely with, their counterparties, including us, which may lengthen sales cycles or increase our costs. Furthermore, if our competitors' ESG performance is perceived to be better than ours, potential or current investors may elect to invest with our competitors instead. In addition,~~ in **this area** ~~the event that we communicate certain initiatives or goals regarding ESG matters~~ , ~~we could fail, or be perceived to fail, in our achievement of such initiatives or goals, or~~ we could be criticized for the ~~scope~~ **accuracy, adequacy, or completeness** of such **disclosures. In addition, we may communicate related goals or** initiatives ~~or~~ **from time to time, which can be costly to achieve and difficult to implement. There is no assurance that we will achieve any of these** goals **, that our initiatives will achieve their intended outcome, and our ability to implement these initiatives or achieve these goals may be dependent on external factors outside our control. Further, we may experience backlash from customers, government entities, advocacy groups, employees, or other stakeholders who disagree with our actual or perceived positions, or with our lack of position on social, environmental, governance, political, public policy, economic, geopolitical, or other sensitive issues. Any perceived lack of transparency about these matters could harm our brand and reputation, our employees' engagement and retention, and the willingness of our customers and partners to do business with us** . Climate change may have an impact on our business. ~~While we seek to mitigate our business risks associated with climate change (such as drought, wildfires, hurricanes, increased storm severity and sea level rise), we recognize that there~~ **There** are inherent climate- related risks wherever business is conducted. ~~Our primary locations may be vulnerable to~~ **We have a global workforce, and operate in leased office spaces and data centers, and** the ~~adverse effects of~~ **short, medium and long term** climate **impacts to** ~~change. For example, certain of~~ our **business** ~~offices have experienced, and~~ are **unclear** ~~projected to continue to experience, climate- related events at an increasing frequency, including drought, heat waves, wildfires and resultant air quality impacts and power shutoffs associated with wildfire prevention~~ . Changing market dynamics, global policy developments and the increasing frequency and impact of extreme weather events **to** ~~on critical~~ infrastructure in the U. S. and elsewhere have the potential to disrupt our business, the business of our third- party suppliers and the business of our customers, and may cause us to experience losses and additional costs to maintain or resume operations. In addition, we may be subject to increased regulations, reporting requirements,

standards or expectations regarding the environmental impacts of our business.