

## Risk Factors Comparison 2025-02-24 to 2024-02-28 Form: 10-K

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

The following are important factors that could cause our actual operating results to differ materially from those indicated or suggested by forward- looking statements made in this annual report on Form 10- K or presented elsewhere by management from time to time. Financial and Operational Risks Slowing revenue growth has in the past and may continue to negatively impact our profitability and stock price. The overall revenue growth we have enjoyed in recent years may not continue in future periods and could decline, which could negatively impact our profitability and stock price. Our ability to generate revenue depends on the amount of services we deliver, continued growth in demand for our security, delivery and compute solutions and our ability to maintain the prices we charge for them. Revenue we generate from our delivery solutions is impacted by pricing pressure due to competition and fluctuations in content traffic as a result of, among other factors, changes in the popularity of our customers' content including video delivery and gaming , **and economic pressures on our customers that can cause them to take steps to optimize their platforms, including through " do- it- yourself", or DIY, initiatives** . For example, revenue from our delivery solutions increased significantly in 2020 due in large part to greater consumption of online media and games during the onset of the COVID- 19 pandemic and the associated stay- at- home orders ~~across the globe~~ . However, as these orders were lifted and more return- to- work policies were adopted, our revenue from delivery solutions declined . **In addition, a large social media company has recently taken steps to lower costs and reduce reliance on U. S. providers, including a DIY component, which we believe is in part a reaction to certain geopolitical pressures, and which has reduced traffic on our network and negatively impacted revenue in 2024. Other customers have and may continue to reduce their traffic with us, negatively impacting revenue** . We have continued to experience revenue declines in our delivery solutions and expect this trend to continue in the near future. Our security solutions currently generate the largest portion of our revenue. Our ability to generate revenue in our security business depends on our ability to increase our industry recognition as a provider of security solutions, develop or acquire new solutions in a rapidly- changing environment where security threats are constantly evolving and ensure that our solutions operate effectively and are competitive with products offered by others. **Further, security revenue for some products is impacted by traffic levels on our network and recently has, and may continue to be, negatively impacted by reduced traffic on our network, including the reduced traffic from a large social media company among other customers.** In addition, an increasing proportion of our revenue has **recently** been generated by our compute solutions. Our ability to generate revenue in our compute business is dependent on our ability to successfully continue building our compute ~~infrastructure~~ **platform** , attract a customer base that has traditionally partnered with more established companies in the compute industry , and develop effective, price competitive and attractive solutions. If we are unable to increase revenues, our profitability and stock price could suffer. See the risk factor titled, " Global conditions have in the past and may in the future harm our industry, business and results of operations" below. Global conditions have in the past and may in the future harm our industry, business and results of operations. We operate globally and as a result, our business, revenues and profitability are impacted by global macroeconomic conditions. The success of our activities is affected by general economic and market conditions, including, among others, inflation, **foreign exchange rates**, interest rates, tax rates, economic uncertainty, political instability, warfare, changes in laws, trade barriers, the actual or perceived failure or financial difficulties of financial institutions, reduced consumer confidence and spending and economic and trade sanctions. **Global economic and geopolitical conditions can impact our customers, causing them to take cost- savings measures that can include optimization and " do- it- yourself", or DIY, initiatives, which can impact our revenues.** For example, ~~approximately 1% of a large social media company has recently taken steps to lower costs and reduce reliance on U. S. providers by optimizing its platform, including a DIY component, which reduced traffic on~~ our 2021 ~~network and negatively impacted our~~ revenue had been generated from traffic into Russia, Belarus and Ukraine, and we experienced a decline in revenue in 2022 and 2023 related to the war in Ukraine due to a decrease in traffic in these countries. In addition, due to changes in international tax laws, we expect ~~our effective income tax rate will increase~~ in 2024. The U. S. capital markets have experienced and may continue to experience extreme volatility and disruption in the recent past. Furthermore, inflation rates in the U. S. have ~~recently been elevated~~ **compared to historical rates and have fluctuated. In addition, the Trump administration has indicated an intention to impose tariffs on certain countries that could adversely impact trade relations, result in higher costs and decreased purchasing power of our customers, put** increased ~~to levels not seen in decades~~ **pressure on supply chains and create general market instability** . Such economic volatility has in the past and could in the future adversely affect our business, financial condition, results of operations and cash flows and future market disruptions could negatively impact us. For example, these unfavorable economic conditions could increase our operating costs, which ~~could negatively~~ **could negatively** impact our profitability. Geopolitical destabilization and warfare have impacted and could continue to impact global currency exchange rates, resources from our suppliers , and our ability to operate or grow our business . ~~In addition, we have recently experienced rising energy costs in areas in which we operate, particularly in Europe~~ . Additionally, we have offices and employees located in regions that historically have and may again experience periods of political instability, warfare, changes in laws, trade barriers and economic and trade sanctions. Adverse conditions in these countries have in the past and may in the future affect our operations, including disruptions to our workforce, supply chains, networks, financial systems and other critical infrastructure, which could adversely affect our business, results of operations, financial condition and cash flows. For example, approximately ~~five~~ **six** percent of our global employees are located in ~~Tel Aviv~~, Israel and some of our employees have been mobilized as members of the Israeli military reserves. ~~The ongoing~~ **Should the Isreal- Hamas** war **continue, it** could cause harm to our

employees or otherwise impair their ability to work for extended periods of time. Failure to control expenses could reduce our profitability, which would negatively impact our stock price. Maintaining or improving our profitability depends both on our ability to increase our revenue and limit our expenses. We base our decisions about expense levels and investments on estimates of our future revenue and future anticipated rates of growth and may incur varying levels of expense based on strategic initiatives, including acquisitions and the build out of our network to support our compute solutions. In addition, many of our expenses are fixed costs for a certain amount of time which may impact our ability to reduce costs in a timely manner or without incurring additional costs. If we are unable to increase revenue and limit expenses, our results of operations will suffer. We have in the past and may in the future take certain steps to reduce expenses, however, there are no assurances that we will be able to effectively reduce our expenses and such actions may negatively affect our ability to invest in our business for innovation, systems improvements and other initiatives. If we do not develop or acquire new solutions that are attractive to our customers, our revenue and operating results could be adversely affected. Innovation is important to our future success. In particular, as security and compute solutions have become, and are expected to continue to be, an important part of our business, we must be particularly adept at developing new security solutions that meet the constantly- changing threat landscape and compute and compute- to- edge solutions that meet the needs of professional users and enterprises looking to increase the utility of the internet for their business. The process of developing new solutions and product enhancements is complex, lengthy and uncertain and has become increasingly complex due to the sophistication of our customers' needs. The development timetable is uncertain and we may commit significant resources to developing solutions for which a viable market may not ultimately develop. For example, ~~with the acquisition of Linode,~~ we are investing significant resources in our compute solutions and platform, working on expanding the capacity of these facilities, adding additional sites and developing increased compute features and functionality. Success in these efforts is not guaranteed and will largely depend on our ability to create products that are competitive in the enterprise market, source additional co- location facilities ~~and,~~ manage an uncertain supply chain for server related hardware **and adapt our offerings to new or emerging technologies and changes in customer requirements, including those related to artificial intelligence workloads.** In addition, we have ~~also~~ experienced, and may in the future experience, delays in developing and releasing new products and product enhancements. This could cause our expenses to grow more rapidly than our revenue. Trying to innovate through acquisition can be costly and with uncertain prospects for success; we may find that attractive acquisition targets are too expensive for us to pursue which could cause us to pursue more time-consuming internal development. Failure to develop, on a cost- effective basis, innovative or enhanced solutions that are attractive to customers and profitable to us could have a material detrimental effect on our business, results of operations, financial condition and cash flows. If we are unable to compete effectively and adapt to changing market conditions, our business will be adversely affected. We compete in markets that are intensely competitive and rapidly changing. Our current and potential competitors vary by size, product offerings and geographic region ~~;~~ and range from start- ups that offer solutions competing with a discrete part of our business to large technology or telecommunications companies that offer, or may be planning to introduce, products and services that are broadly competitive with what we do. The primary competitive factors in our market are differentiation of technology, global presence, quality of solutions, **reliability,** long- term product roadmap, customer service, technical expertise, security, ease- of- use, breadth of services offered, price and financial strength. Many of our current and potential competitors have substantially greater financial, technical and marketing resources, larger customer bases, broader product portfolios, longer operating histories, greater brand recognition and more established relationships in the industry than we do. This is particularly true with respect to our compute solutions, as a small number of very large competitors have established themselves as leaders in the compute business. As a result, some competitors **have in the past and may in the future** be able to: develop superior products or services; leverage better name recognition, particularly in the security and compute markets; enter new markets more easily or better manage the impact of changes in general economic conditions, geopolitical conditions and industry pressures; gain greater market acceptance for their products and services; enter into long- term contracts with our potential customers; increase their points of presence and proximity to enterprise data centers and end users faster than us; expand their offerings more efficiently and more rapidly; bundle their products that are competitive with ours with other solutions they offer in a way that makes our offerings less appealing to, or more costly for, current and potential customers; more quickly adapt to new or emerging technologies and changes in customer requirements; take advantage of acquisition, investment and other opportunities more readily; offer lower prices than ours, including at levels that may not be profitable for us to match; spend more money on the promotion, marketing and sales of their products and services; offer higher salaries to talented professionals which may impact our ability to hire or retain engineering and other personnel; and implement shorter sales cycles with customers and prospects. Smaller and more nimble competitors may be able to: attract customers by offering less sophisticated versions of products and services than we provide at lower prices than those we charge; develop new business models that are disruptive to us; and respond more quickly than we can to new or emerging technologies, changes in customer requirements and market and industry developments, resulting in superior offerings. Ultimately, any type of increased competition could result in price and revenue reductions, loss of customers and loss of market share or inability to penetrate new markets, each of which could materially impact our business, profitability, financial condition, results of operations and cash flows. We and other companies that compete in this industry and these markets experience continually shifting business relationships, reputations, commercial focuses and business priorities, all of which occur in reaction to industry and market forces and the emergence of new opportunities. These shifts have led or could lead to our customers or partners becoming our competitors; **customers implementing multi- vendor policies and seeking out one or more of our competitors to provide content and application delivery or security protection services;** network suppliers no longer seeking to work with us; and technology companies that previously did not appear to show interest in the markets we seek to address entering into those markets as our competitors. With this constantly changing environment, we may face operational difficulties in adjusting to the changes or our core strategies could become obsolete. Any of these or other developments could harm our business. Defects or

disruptions in our products and IT systems could require us to increase spending on upgrading systems, diminish demand for our solutions or subject us to substantial liability. Our solutions are highly complex and are designed to be deployed in and across numerous large and complex networks that we do not control. From time to time, we have needed to correct errors and defects in the proprietary and open- source software that underlies our platform that have given rise to service incidents, outages and disruptions or otherwise impacted our operations. We **have in the past and** could **in the future** face the loss of customers from these incidents as they seek alternative or supplemental providers. We have also periodically experienced customer dissatisfaction with the quality of some of our delivery, security, compute and other services, which has led to a loss of business and could lead to a loss of customers in the future. Furthermore, most of our customer agreements contain service level commitments. If we fail to meet these contractual commitments, we could be obligated to provide credits for future service, or face contract termination with refunds of prepaid amounts, which could harm our business. We may not have in place adequate quality assurance procedures to ensure that we detect errors in our hardware, software and open- source components **that** we use in a timely manner, and we may have insufficient resources to efficiently address multiple service incidents happening simultaneously or in rapid succession. If we are unable to efficiently and cost- effectively fix errors or other problems that we identify and improve the quality of our solutions or systems, or if there are unidentified errors that allow persons to improperly access our services or systems, we could experience litigation, the need to issue credits to customers, loss of revenue and market share, damage to our reputation, diversion of management attention, increased expenses, reduced profitability and other negative consequences which could harm our business. Defects in our security solutions **or human error** could lead to negative publicity, loss of business, damages payments to customers, diminishing customer appeal and other negative consequences which could harm our business. As our solutions are adopted by an increasing number of enterprises and governments, it is possible that the adversaries behind advanced malicious actions will specifically focus on finding ways to defeat our products and services. If they are successful, we could experience a serious impact on our reputation and financial condition as a provider of security solutions. We are devoting significant resources to develop and deploy our own competing **cloud computing compute** offering. The rapid development and deployment of new compute infrastructure bears the risk of bugs and unforeseen failures that could affect our reputation and ability to execute our strategies. The risks of such bugs and unforeseen failures introduced to our compute **infrastructure platform** by our customers who control many aspects of their use of our compute services and experimental technologies could affect our reputation **and**, ability to execute our strategies **and our financial condition**. It is also uncertain whether our strategies to develop and deploy our own competing **cloud computing compute** offering will attract **the additional** customers or generate **the enough** revenue required to be successful. **These** **The** costs **related to these efforts** may **also** reduce the gross and operating margins we have previously achieved. Failure to adequately and rapidly deploy additional points of presence, increased proximity to enterprise data centers and end users and develop competitive offerings could result in negative publicity, loss of business, diminishing customer appeal and other negative consequences which could harm our business. Our business relies on our data systems, traffic measurement systems, billing systems, ordering processes and other operational and financial reporting and control systems. We also rely on third- party software for certain essential operational services and a failure or disruption in these services could materially and adversely affect our ability to manage our business effectively. All of these systems have become increasingly complex due to the complexity of our business, use of third- party software and services, acquisitions of new businesses with different systems **and increased changing** regulation over controls and procedures. As a result, these systems have in the past and could in the future generate errors that impact traffic measurement or invoicing, revenue recognition and financial forecasting or other parts of our business. We will need to continue to upgrade and improve our data systems, traffic measurement systems, billing systems, ordering processes and other operational and financial systems, procedures and controls. These upgrades and improvements may be difficult and costly. If we are unable to adapt our systems and organization in a timely, efficient and cost- effective manner to accommodate changing circumstances, our business may be adversely affected. Cybersecurity breaches and attacks on us, our contractors or our third- party vendors, as well as steps we need to take in an effort to prevent them, can lead to significant costs and disruptions that would harm our business, financial results and reputation. We regularly face attempts to gain unauthorized access or deliver malicious software to Akamai **Connected Cloud's platforms, products and services** and our internal IT systems, with the goal of stealing proprietary information related to our business, products, employees and customers; disrupting our systems and services or those of our customers or others; or demanding ransom to return control of such systems and services. These attempts take a variety of forms, including Distributed Denial of Service ( **" DDoS "**) attacks, infrastructure attacks, botnets, malicious file uploads, application abuse, credential abuse, social engineering, ransomware, bugs, viruses, worms and malicious software programs. Additionally, the use of artificial intelligence by bad actors has heightened the sophistication and effectiveness of these types of attacks **, and may be used to create attacks that current processes and technologies are unable to adequately address**. There have in the past and could in the future be attempts to infiltrate our systems through our supply chain and contractors. Malicious actors are known to attempt to fraudulently induce employees and suppliers to disclose sensitive information through illegal electronic spamming, phishing or other tactics. Other parties may attempt to gain unauthorized physical access to our facilities in order to infiltrate our internal- use information systems. Furthermore, nation state and hacktivist attacks against us or our customers **have in the past and** may **in the future** intensify during periods of heightened geopolitical tensions or armed conflict, such as the ongoing war in Ukraine and the Israel- Hamas War. We may not be able to anticipate the techniques used in such attacks, as they change frequently and may not be recognized until launched **. The rapidly changing geopolitical landscape may also create new, unexpected, or unknown risks for which we may not immediately be prepared, requiring increased risk mitigation expenditures**. While we have, from time to time, experienced threats to and breaches of our and our third- party vendors' data and systems, to date, to our knowledge, cyber threats and other attacks have not resulted in any material adverse effect to our business or operations, but such threats are constantly evolving, increasing the difficulty of detecting and successfully defending against them. The complexities in

managing the security profile of a distributed network with vast scale and geographic reach that evolves to incorporate new capabilities expose us to both known and unknown vulnerabilities. We have discovered vulnerabilities in software **and hardware** used in our technology, such as the **AMD" Inception"** vulnerability in Apache Log4j 2 referred to as "Log4Shell" identified in **late mid- 2021-2023** that **potentially** impacted a large portion of the internet ecosystem, and may have other undiscovered vulnerabilities. Vulnerabilities, resident in **either software , hardware** or configurations, **have in the past and may in the future** require significant operational efforts to mitigate and may persist for extended periods of time and the effects of any such vulnerability could be exacerbated. Similar security risks exist with respect to acquired companies, our business partners and the third- party vendors that we rely on for aspects of our information technology support services and administrative functions. As a result, we are subject to risks that the activities of our business partners and third- party vendors may adversely affect our business even if an attack or breach does not directly target our systems. To protect our corporate and deployed networks, we aim to continuously engineer more secure solutions, enhance security and reliability features, improve the deployment of software updates to address security vulnerabilities, develop mitigation technologies that help to secure customers from attacks and maintain the digital security infrastructure that protects the integrity of our network and services. For example, our ongoing efforts to continually enhance the security and reliability of **Akamai Connected Cloud our globally distributed infrastructure**, customer applications and corporate systems comprise various initiatives and mitigation efforts, including ~~;~~but not limited to ~~;~~upgrading access and configuration controls; improving security instrumentation, monitoring, detection and prevention tools; enhancing software inventory and tracking and patching systems; upgrading encryption processes and protections; enhancing authorization methods in applications; enhancing data loss prevention and endpoint security management capabilities; upgrading vulnerability identification, assessment and remediation processes and technologies; and enhancing the security of passwords and other credentials, as applicable and appropriate. Our efforts to engineer more secure solutions are frequently costly, with a negative impact on near- term profitability, and may be unsuccessful in preventing security incidents that may have an adverse effect on our business and reputation. For example, with the acquisition of Linode, we ~~are continue to adapting~~ **adapt** procedures for mitigating risks that have in the past or may in the future materialize, including any harms that may arise from abuse of our compute products. If we fail to mitigate these harms or if there is a significant cybersecurity event using our compute products or our compute products are perceived to be less reliable than our competitors, it could result in loss of customers and reputational damage. Any actual, alleged or perceived breach of network security in our systems or networks, or any other actual, alleged or perceived compromise or data security incident we, our customers or our third- party suppliers suffer, ~~can~~ **has in the past and could in the future** result in damage to our reputation; negative publicity; loss of channel partners, customers and sales; loss of revenue; loss of competitive advantages; increased costs to remedy any problems and otherwise respond to any incident; regulatory investigations and enforcement actions and fines; costly litigation; and other liabilities. If we cannot maintain compatibility with our customers' IT infrastructure, including their chosen third- party ~~applications~~ **services**, our business will be harmed. Our products interoperate with our customers' IT infrastructures that often have different specifications, utilize diverse technology and require compatibility with multiple communication protocols. Therefore, the functionality of our technology often needs to have, and maintain, compatibility with our customers' technology environment, including their chosen third- party technology. Aspects of our technology' s compatibility with our customers' technology is dependent on our customers because our customers, and in particular those who implement third- party applications within their environments, may change features, restrict our access to, or alter their applications within their discretion and in a manner that causes incompatibilities or causes us significant costs to maintain compatibility. Such changes could functionally limit or prevent the compatibility of our products with our customers' IT infrastructure, which would negatively affect adoption of our products and harm our business. If we fail to update our products to achieve compatibility with new third- party applications that our customers use, we may not be able to offer the functionality that our customers need, which would harm our business. We face risks associated with global operations that could harm our business. A significant portion of our hiring, new customers and revenue growth in recent ~~quarters~~ **years** has been attributable to our business outside the U. S. Our operations in international countries subject us to risks that may increase our costs, impact our financial results, disrupt our operations or make our operations less efficient and require significant management attention. These risks include: foreign exchange rate risks; uncertainty regarding liability for content or services, including uncertainty as a result of local laws and lack of legal precedent; loss of revenues if the U. S. or international governments impose limitations on doing business with significant current or potential customers; difficulty in staffing, training, developing and managing international operations as a result of distance, language, cultural differences, differences in employee / employer relationships or regulations; theft of intellectual property in high- risk countries where we operate; difficulties in enforcing contracts, collecting accounts and longer payment cycles in certain countries; difficulties in transferring funds from, or converting currencies in, certain countries; managing the costs and processes necessary to comply with export control, sanctions, such as the sanctions imposed in connection with the Russian invasion of Ukraine, anti- ~~corruption~~ **bribery**, data protection, cybersecurity and competition laws and regulations or other regulatory or contractual limitations on our ability to sell or develop our products and services in certain international markets; macroeconomic developments and changes in the labor markets in which we operate; geopolitical developments, including any that impact our or our customers' ability to operate in or deliver content to a country; other circumstances outside of our control such as trade disputes, **including the imposition of tariffs by the United States on imports from certain countries and any resulting counter- tariffs or macroeconomic impacts**, political unrest, warfare, military or armed conflict, such as the Russian invasion of Ukraine and the ~~ongoing~~ Israel- Hamas War, terrorist attacks, public health emergencies, energy crises and natural disasters that could disrupt our ability to provide services or limit customer purchases of them. For example, approximately ~~five~~ **six** percent of our global employees are located in ~~Tel Aviv~~, Israel and have been and may continue to be impacted by the Israel- Hamas War. A number of our employees have been, and more may be, required to report for military duty which could impact our ability to operate and successfully complete

ongoing initiatives particularly with respect to our security offerings and our efforts to move our internal applications from third-party clouds to Akamai Connected Cloud. In addition, further attacks by Hamas or our compute platform other groups on Israel could further impact our workforce, our operations and our offices located in Tel Aviv. Furthermore, a widening of the conflict in the Middle East or further escalation could lead to broader geopolitical destabilization and macro- economic impacts. In addition, we are subject to laws and regulations worldwide that differ among jurisdictions, affecting our operations in areas such as intellectual property ownership and infringement; tax; anti- ~~corruption-bribery~~ ; internet and technology regulations; so-called " fair share" or internet content taxes; foreign exchange controls and cash repatriation; data privacy; cyber security; competition; consumer protection; **corporate sustainability**; and employment. Compliance with such requirements can be onerous and expensive and may otherwise impact our business operations negatively. Although we have policies, controls and procedures designed to help ensure compliance with applicable laws, there can be no assurance that our employees, contractors, suppliers, customers or agents will not violate such laws or our policies. Violations of these laws and regulations can result in fines; additional costs related to governmental investigations; criminal sanctions against us, our officers or our employees; prohibitions on the conduct of our business; and damage to our reputation. Our business strategy depends on the ability to source adequate transmission capacity, co- location facilities and the equipment we need to operate our network; failure to have access to those resources could lead to loss of revenue and service disruptions. To operate and grow our **globally distributed network serving our portfolio of services**, we are dependent in part upon transmission capacity provided by third- party telecommunications network providers, the availability of co- location facilities to house our servers and equipment to support our operations. We may be unable to purchase the bandwidth and space we need from these providers due to limitations on their resources, increasing energy costs or other reasons outside of our control. In particular, ~~following our acquisition of Linode,~~ our efforts to increase the size and scale of our ~~compute solutions~~ **network infrastructure** have required and may continue to require procuring significant additional space in co- location facilities. Inability to access facilities where we would like to install servers, or perform maintenance on existing servers for any reason ~~;~~ impedes our ability to expand or maintain capacity. As a result, there can be no assurance that we are adequately prepared for unexpected increases in capacity demands by our customers ~~;~~ particularly those under cyber- attack or impacted by geopolitical conditions, such as the ongoing war in Ukraine or the Israel- Hamas War. Failure to put in place the capacity we require to operate our business effectively could result in a reduction in, or disruption of, service to our customers and ultimately a loss of those customers. Akamai ~~Connected Cloud~~ **relies 's platforms, products and services rely** on hardware equipment, including hundreds of thousands of servers deployed around the world. Disruptions in our supply chain have occurred in the past and could prevent us from purchasing needed equipment at attractive prices or at all. For example, **we are experiencing continued volatility in certain server component costs that support the continued build out of our compute platform. In addition,** from time to time, it has been, and may continue to be, more difficult to purchase equipment that is manufactured in areas that face disruptions to operations due to unrest, trade sanctions or other political activity, public health issues, safety issues, natural disasters or general economic conditions. **For example, tariffs imposed by the United States on other countries and any resulting counter- tariffs will likely lead to increasing costs and supply chain disruptions.** Failure to have adequate equipment, including server **and other networking** equipment, could harm the quality of our services, which could lead to the loss of customers and revenue. Acquisitions and other strategic transactions could result in operating difficulties, dilution, diversion of management attention and other harmful consequences that may adversely impact our business and results of operations. We expect to continue to pursue acquisitions and other types of strategic relationships that involve technology sharing or close cooperation with other companies. Acquisitions and other complex transactions are accompanied by a number of risks, including the following: difficulty integrating technologies, operations and personnel while maintaining the quality standards ~~that are consistent with our reputation~~ ; potential disruptions of our ongoing business and distraction of management attention; diversion of financial and business resources from core operations or other attractive investments; financial consequences, such as increased operating expenses, incurrence of material post- closing liabilities, incurrence of additional debt and other dilutive effects on our earnings, particularly in the current environment where we have seen relatively high valuations of, and valuation expectations for, many technology companies and increasing allocation of risk to acquirors; failure to realize synergies or other expected benefits; lawsuits resulting from an acquisition or disposition; the inability to retain the acquired company' s key talent; exposure to cybersecurity risks and the cost associated with remediating those risks in connection with the acquisition of IT systems; increased accounting charges such as impairment of goodwill or intangible assets, amortization of intangible assets acquired and a reduction in the useful lives of intangible assets acquired; the need to use substantial portions of available cash or dilutive issuances of securities to finance large transactions; and potential unknown liabilities and regulatory requirements associated with an acquired business. The data practices and technology systems of businesses that we have acquired, or may acquire, and our efforts to integrate our acquisitions with our existing technologies have in the past and may in the future pose risks, such as cybersecurity vulnerabilities or past cybersecurity or privacy incidents. Following an acquisition, we work to enhance the security and reliability of our systems. As such, there is a period of increased cybersecurity risk during the period between closing an acquisition and the completion of our security upgrades and integration. For example, as part of the integration of the Linode compute platform into Akamai ~~Connected Cloud~~ **'s platform** and the migration of certain applications and products from third party cloud providers onto Akamai ~~Connected Cloud~~ **'s compute platform**, we have been working to enhance the security and reliability of the integrated systems. While we continue to make progress on these efforts, the mitigation of a number of risks is ongoing and thus certain underlying vulnerabilities remain that, if exploited, could negatively impact Akamai ~~Connected Cloud~~ **'s platform** and our customers. Despite our efforts to enhance the security and reliability of our systems, our information technology systems and those of third parties with whom we do business or communicate may be damaged, disrupted, or shut down due to attacks by unauthorized access, malicious software, computer viruses, undetected intrusion, hardware failures, or other events. In addition, our disaster recovery plans may be ineffective or inadequate. Any inability to

integrate completed acquisitions or combinations in an efficient and timely manner could have an adverse impact on our results of operations. If current and potential large customers shift to ~~hardware-based or other~~ DIY internal solutions for content and application delivery or security protection, our business will be negatively impacted. We are reliant on some of our larger customers to direct traffic to our network for a significant part of our revenues. **At times** ~~In the past~~, some of our customers have determined that it is better for them to employ a “do-it-yourself” or “DIY” strategy by putting in place equipment, software and other technology solutions for content and application delivery and security protection within their internal systems instead of using our solutions for some or all of their needs. As the amount of money a customer spends with us increases, the risk that they will seek alternative solutions such as DIY or a multi-vendor policy likewise increases. While the number of customers implementing a DIY strategy **had been decreasing, current global economic and geopolitical conditions may cause customers to increase their focus on DIY solutions, which could negatively impact traffic on our network, and, as a result, our revenue. For example, a large social media customer has decreased in recent-recently years taken steps to lower costs and reduce reliance on U. S. providers by optimizing its platform, including using a DIY component, which has reduced traffic on our network and negatively impacted our revenue in 2024 and is likely to continue to do so in the future. If our customers increase their use of DIY solutions or** if multiple **additional** large customers shift to this model, traffic on our network and our contracted revenue commitments ~~would~~ **could** decrease **more significantly**, which ~~would~~ **could** negatively impact our business, profitability, financial condition, results of operations and cash flows. If we are unable to recruit and retain key employees and qualified sales, research and development, technical, marketing and support personnel, our ability to compete could be harmed. Our future success depends upon the services of our executive officers and other key technology, sales, research and development, marketing and support personnel who have critical industry experience and relationships. **Attracting** ~~Like other companies in our industry, we have experienced difficulty in hiring and retaining highly skilled and qualified employees with appropriate qualifications, continues to be a priority and ; if a key dependency for our ongoing success. If~~ we fail to attract new personnel ~~or~~, fail to retain and motivate our current personnel or **fail to** effectively train our ~~current~~ employees to support our business needs, our business and future growth prospects could suffer. For example, none of our officers or key employees **is are** bound by an employment agreement for any specific term, and members of our senior management have left our company over the years for a variety of reasons. In addition, effective succession planning is important to our long- term success and our failure to ensure effective transfer of knowledge and smooth transitions involving our officers and other key personnel could hinder our strategic planning and execution. In addition, our future success will depend upon our ability to attract, train and retain employees, particularly in our expected areas of growth such as security and cloud computing. Such efforts will require time, expense and attention by our employees as there is significant competition for talented individuals. This competition results in increased costs in the form of cash and stock- based compensation and can have a dilutive impact on our stock. In addition, our ability to hire and retain employees may be adversely affected by volatility in the price of our stock or our ability to obtain shareholder approval to offer additional stock to our employees, because a significant portion of our compensation is in the form of equity grants. **We** ~~In addition, we~~ are retasking certain employees to work on our compute solutions which will require the use of our resources and if we are unable to successfully retrain our employees, our compute business may suffer. Furthermore, geopolitical events may impact our retention efforts. For example, the ~~ongoing~~ Israel- Hamas War has and could continue to impact our workforce in ~~Tel Aviv~~, Israel as employees have been and may continue to be required to report for military service or have other competing priorities. The loss of the services of a significant number of our employees or any of our key employees or our inability to attract and retain new talent in a timely fashion may be disruptive to our operations and overall business. Our failure to maintain our company culture and manage new risks as our business evolves and our work practices change could harm us. We believe our culture has been a key contributor to our success to date. As a result of the diversification of our business, personnel growth, the deployment of our FlexBase program, acquisitions and international expansion in recent years, ~~many~~ **most** of our employees are now based outside of our Cambridge, Massachusetts headquarters. If we are unable to appropriately increase management depth, enhance succession planning and decentralize our decision- making at a pace commensurate with our actual or desired growth rates, we may not be able to achieve our financial or operational goals. It is also important to our continued success that we hire qualified personnel, properly train them and manage poorly- performing personnel, all while maintaining our corporate culture and spirit of innovation. If we are not successful in these efforts, our growth and operations could be adversely affected. We rolled out our FlexBase program in May 2022, which allows the more than 95 % of our workforce designated as flexible to choose to work from an Akamai office, their home office, **an approved workspace**, or a combination of ~~both~~ **all three**. This program could, among other things, negatively impact employee morale and productivity, inhibit our ability to effectively train new employees and impede our ability to support customers at the levels they expect. In addition, certain security systems in homes or other remote workplaces may be less secure than those used in our offices, which may subject us to increased security risks, including cybersecurity- related events, and expose us to risks of data or financial loss and associated disruptions to our business operations. Members of our workforce who access company data and systems remotely may not have access to technology that is as robust as that in our offices, which could cause the networks, information systems, applications and other tools available to those remote workers to be more limited or less reliable than in our offices. We may also be exposed to risks associated with the locations of remote workers, including compliance with local laws and regulations or exposure to compromised internet infrastructure. Further, if employees fail to inform us of changes in their work location, we may be exposed to additional risks without our knowledge. If we are unable to effectively maintain a hybrid workforce, manage the cybersecurity and other risks of remote work and maintain our corporate culture and workforce morale, our business could be harmed or otherwise negatively impacted. Our restructuring and reorganization activities may be disruptive to our operations and harm our business. Over the past several years, we have implemented internal restructurings and reorganizations designed to reduce the size and cost of our operations, improve operational efficiencies and reprioritize investments, enhance our ability to pursue market opportunities and

accelerate our technology development initiatives. In February 2021, we announced a significant reorganization to create two new business groups linked to our security and edge delivery technologies as well as establishing a unified global sales force. During the first quarter of 2023 and the third quarter of 2024, management committed to an action actions to restructure certain parts of the company Company, including reducing headcount, to enable it to prioritize investments in the fastest growing areas of the business and redeploy resources to support the Company's strategic investments. We may take similar steps in the future as we seek to realize operating synergies, optimize our operations to achieve our target operating model and profitability objectives, respond to market forces or better reflect changes in the strategic direction of our business. Disruptions in operations may occur as a result of taking these actions. Taking these actions may also result in significant expense for us, including with respect to workforce reductions, as well as decreased productivity due to employee distraction and unanticipated employee turnover. Substantial expense or business disruptions resulting from restructuring and reorganization activities could adversely affect our operating results. We may have exposure to greater- than- anticipated tax liabilities. Our future income taxes could be adversely affected by earnings being lower than anticipated in jurisdictions that have lower statutory tax rates and higher than anticipated in jurisdictions that have higher statutory tax rates, or changes in tax laws, regulations or accounting principles, as well as certain discrete items such as equity- related compensation. The In particular, the Organisation for Economic Co- operation and Development (" OECD ") and participating OECD member countries continue to work toward the enactment of a 15 % global minimum corporate tax rate for large companies with revenue above € 750 million, calculated on a country- by- country basis. European Union member states have begun to enact global minimum tax rate rules into domestic law. In particular, on December 16, 2022, the Swiss parliament approved a constitutional amendment to implement the global minimum tax rate rules and the amendment was approved by public vote on June 18, 2023. On December 22, 2023, the Swiss Federal Council declared some of the rules to be in effect beginning in 2024. The global minimum tax is a significant structural change to the international tax framework, which is expected to affect the tax position of multinational or large scale domestic enterprise groups, also known as " Pillar Two". Many of the participating countries have enacted legislation that became effective fall under its scope, including us, beginning in 2024, while - Although enactment of the other global minimum tax has begun, the OECD and participating OECD member countries continue to work towards on defining the underlying rules and administrative procedures. Although We will continue to monitor these -- the developments enacted and evaluate the impact effective legislation in some countries was applicable to us as of January 1 the global minimum tax, 2024, and which we anticipate will increase increased our liability for corporate taxes and our effective income tax rate, the increase did not have a material impact on our overall results of operations or cash flows. We will continue to monitor and evaluate the impacts of the developing legislation. We have recorded certain tax reserves to address potential exposures involving our income tax and indirect tax positions. These potential tax liabilities result from the varying application of statutes, rules, regulations and interpretations by different jurisdictions. We are currently subject to tax audits in various jurisdictions. If the ultimate outcome of any tax audits are adverse to us, our reserves may not be adequate to cover our total actual liability, and we would need to take a financial charge. Although we believe our estimates, our reserves and the positions we have taken in all jurisdictions are reasonable, the ultimate tax outcome may differ from the amounts recorded in our financial statements and may materially affect our financial results in the period or periods for which such determination is made. - The Inflation Reduction Act of 2022 (" IRA ") includes a 15 % corporate alternative minimum tax for companies with modified GAAP net income in excess of \$ 1 billion, a 1 % excise tax on certain stock repurchases, and numerous environmental and green energy tax credits. Currently, we are not subject to the corporate alternative minimum tax. The impact of the excise tax on our stock repurchase program was immaterial for the year ended December 31, 2023. Fluctuations in foreign currency exchange rates affect our reported operating results in U. S. dollar terms. Because we conduct a substantial portion of our business outside the United States, we face exposure to adverse movements in foreign currency exchange rates, which could have a material adverse impact on our financial results and cash flows. These exposures may change over time as business practices evolve and economic conditions change. The fluctuations of currencies in which we conduct business can both increase and decrease our overall revenue and expenses for any given period. This exposure is the result of selling in multiple currencies, headcount in foreign locations and operating in countries where the functional currency is the local currency. Revenue generated and expenses incurred by our international subsidiaries are often denominated in their local currencies, but many of our expenses related to our operations in foreign jurisdictions are denominated in U. S. dollars. As a result, our consolidated U. S. dollar financial statements are subject to fluctuations due to changes in exchange rates as the financial results of our international subsidiaries are translated from local currencies into U. S. dollars. For example, in 2023 2024, the strength of the U. S. dollar had a negative impact on our revenue and a positive impact on our operating expenses. In addition, our financial results are subject to changes in exchange rates that impact the settlement of transactions in non- functional currencies. In addition, we have recently experienced increased volatility in foreign currency exchange rates, due to a number of factors, including geopolitical and economic developments. We may not be able to effectively manage such volatility, and our financial results have in the past and could in the future be adversely impacted as a result of such volatility. In addition, such volatility, even when it increases our revenues or decreases our expenses, impacts our ability to accurately predict our future results and earnings. Our sales to government clients subject us to risks, including early termination, audits, investigations, sanctions and penalties. We have customer contracts with the U. S. government, as well as international, state and local governments and their respective agencies, and we may in the future increase sales to government entities. Sales to government entities are subject to a number of risks. Selling to government entities can be highly competitive, expensive, and time consuming, often requiring significant upfront time and expense without any assurance that these efforts will generate a sale. Such government entities often have the right to terminate these contracts at any time, without cause. There is increased pressure for governments and their agencies, both domestically and internationally, to reduce spending and demand and payment for our services may be impacted by public sector budgetary cycles and funding authorizations. These factors may

combine to potentially limit the revenue we derive from government contracts in the future. Additionally, government contracts generally have requirements that are more complex than those found in commercial enterprise agreements and therefore are more costly to comply with. Such contracts are also subject to audits and investigations that could result in civil and criminal penalties and administrative sanctions, including contract termination, fee refunds, forfeiture of profits, suspension of payments, fines and suspensions or debarment from future government business. We utilize third- party technology in our business, and failures or vulnerabilities, and / or litigation, related to these technologies may adversely affect our business. We utilize third- party technology software, services and other technology to operate critical functions of our business, including the integration of certain of these technologies into our network, products and services. If these software, services, or other technology become unavailable, malfunction or contain vulnerabilities, our expenses could increase and our ability to operate our network, provide our products and our results of operations could be impaired until equivalent software, technology, or services are purchased or developed or any identified vulnerabilities or malfunctioning are remedied. If we are unable to procure the necessary third- party technology we may need to acquire or develop alternative technology, or we may have to resort to utilizing alternative technology of lower quality. This could limit and delay our ability to offer new or competitive products and increase our costs of production. As a result, our business could be significantly harmed. In addition, the use of third- party technology may expose us to third- party claims of intellectual property infringement which could cause us to incur significant costs in defense or alternative sourcing. We rely on certain “ open- source ” software, which may contain security flaws or other deficiencies, and the use of which could result in our having to distribute our proprietary software, including source code, to third parties on unfavorable terms, either of which could materially affect our business. Certain of our offerings use software that is subject to open- source licenses. Open- source code is software that is freely accessible, usable and modifiable; however, certain open- source code is governed by license agreements, the terms of which could require users of such software to make any derivative works of the software available to others on unfavorable terms or at no cost. Because we use open- source code, we may be required to take remedial action in order to protect our proprietary software. Such action could include replacing certain source code used in our software, discontinuing certain of our products or taking other actions that could be expensive and divert resources away from our development efforts. In addition, the terms relating to disclosure of derivative works in many open- source licenses are unclear and have not been interpreted by U. S. courts. If a court interprets one or more such open- source licenses in a manner that is unfavorable to us, we could be required to make certain of our key software generally available at no cost. We could also be subject to similar conditions or restrictions should there be any changes in the licensing terms of the open- source software incorporated into our products. In either event, we could be required to seek licenses from third parties in order to continue offering our products, to re- engineer our products or to discontinue the sale of our products in the event re- engineering cannot be accomplished on a timely or successful basis, any of which could adversely affect our business, operating results and financial condition. Furthermore, open- source software may have security flaws and other deficiencies that could make our solutions less reliable and damage our business. **We may not be successful in our artificial intelligence initiatives, which could adversely affect our business, reputation, or financial results. Artificial intelligence (" AI"), presents new risks and challenges that may affect our business. We have made, and expect to continue to make investments to integrate AI and machine learning technology into our products and solutions. Given the nature of AI technology, we face significant competition from other companies and an evolving regulatory landscape. Our AI efforts may not be successful and our competitors may incorporate AI into their products more successfully than us, which could impair our ability to compete effectively and adversely affect our financial results. The rapid evolution of AI combined with the uncertain and often inconsistent regulatory landscape may require significant additional resources and costs and could in some cases limit our ability to implement AI capabilities in our solutions or to use AI to support business operations. Further, data used to train AI- based systems may lead to harm to our reputation. Despite our implementation of programs designed to support responsible AI use and development, we may not successfully address all issues that may arise. For example, privacy concerns, user consent, supply chain security, transparency and the accuracy, completeness and suitability of data sets are all potential issues that could adversely affect our business, reputation, or financial results**

. Legal and Regulatory Risks Evolving privacy regulations could negatively impact our profitability and business operations. The nature and breadth of laws and regulations, or expanded interpretation of these laws and regulations, that relate to privacy on the internet and international data transfer restrictions may increase in the future. Accordingly, we are unable to assess the possible effect of compliance with future requirements or whether our compliance efforts will materially impact our business, results of operations or financial condition, as well as increase expenses or create other disadvantages to our business. Privacy laws are rapidly proliferating, changing and evolving globally. Governments, private citizens and privacy advocates with class action attorneys are increasingly scrutinizing how companies collect, process, use, store, share and transmit personal data. Numerous laws, such as the European Union' s General Data Protection Regulation (" GDPR"), and the California Consumer Privacy Act of 2018 (" CCPA"), and industry self- regulatory codes have been enacted, and more laws are being considered that may affect how we use data generated from our network as well as our ability to reach current and prospective customers, understand how our solutions are being used and respond to customer requests allowed under the laws. Any perception that our business practices, our data collection activities or how our solutions operate represent an invasion of privacy or improper practice, whether or not consistent with current regulations and industry practices, may subject us to public criticism or boycotts, class action lawsuits, reputational harm, or actions by regulators, or claims by industry groups or other third parties, all of which could disrupt our business and expose us to liability. Engineering efforts to build new capabilities to facilitate compliance with increasing international data transfer restrictions and new and changing privacy laws and related customer demands could require us to take on substantial expenses and divert engineering resources from other projects. We might experience reduced demand for our offerings if we are unable to engineer products that meet our legal duties or help our customers meet their obligations under the GDPR, the CCPA or other applicable data regulations, or if the changes we implement to comply with

such laws and regulations make our offerings less attractive. Our ability to leverage the data generated by our global networks is important to the value of many of the solutions we offer, our operational efficiency and future product development opportunities. Our ability to use data in this way may be constrained by regulatory developments. Compliance with applicable laws and regulations regarding personal data may require changes in services, business practices or internal systems that result in increased costs, lower revenue, reduced efficiency or greater difficulty in competing with other companies. Compliance with data regulations might limit our ability to innovate or offer certain features and functionality in some jurisdictions where we operate. Failure to comply with existing or new rules may result in significant penalties or orders to stop the alleged non-compliant activity, as well as negative publicity and diversion of management time and effort. Our security controls over personal data, our training of employees and third parties on privacy, data security and other ethical data use practices we follow may not prevent the improper disclosure or misuse of customer or end-user data we process. Improper disclosure or misuse of personal data could harm our reputation, lead to legal exposure to customers or end users, or subject us to liability under laws that protect personal data, resulting in increased costs or loss of revenue. Other regulatory developments could negatively impact our business. U. S. and international laws and regulations that apply to the internet related to, among other things, content liability, security requirements, law enforcement access to information, critical infrastructure, net neutrality, so-called "fair share" or internet content taxes, international data transfer restrictions, sanctions, export controls and restrictions on social media or other **platforms, applications or** content could pose risks to our revenues, intellectual property and customer relationships as well as increase expenses or create other disadvantages to our business. Section 230 of the U. S. Communications Decency Act, often referred to as Section 230, gives websites that host user-generated content broad protection from legal liability for content posted on their sites. Proposals to repeal or amend Section 230 could expose us to greater legal liability in the conduct of our business. Our Acceptable Use Policy prohibits customers from using our network to deliver illegal or inappropriate content; if customers violate that policy, we may nonetheless face reputational damage, enforcement actions or lawsuits related to their content. **Further, laws and Regulations regulations related to have been enacted or proposed in a number of countries that limit the delivery of certain types of content into those countries. Enactment and expansion of such laws and regulations would negatively impact our revenues. For example, restrictions were adopted in India in 2020 prohibiting access to identified Chinese applications, which caused a reduction in revenue to us. In addition, such laws and regulations could cause internet service providers, or others, to block our products in order to enforce content-blocking efforts. In addition, efforts Efforts to block a single product or domain name may end up blocking a number of other products or domain names in an overbroad manner that could affect our business. Regulations have also been enacted or proposed in a number of countries that limit the delivery of certain types of content into those countries. Enactment and expansion of such laws and regulations would negatively impact our revenues. For example, restrictions were adopted in India in 2020 prohibiting access to identified Chinese-owned applications which caused a reduction in revenue to us. In addition, in April 2024, the U. S. government passed legislation that prohibited the provision of certain types of services to regulations related a Chinese application if the application was not sold to a neutral third party by January 19, 2025. The Chinese application was not sold to a neutral third party by the January 19th deadline, but President Trump subsequently signed an executive order instructing the U. S. Attorney General to not take any action to enforce the passed legislation for a period of 75 days from January 20, 2025. The Attorney General has since determined that our provision of services to this customer has not violated the law and that we can continue providing services as contemplated by the Executive Order without violating the law and without incurring any legal liability. In the past year, this customer has taken steps to lower costs and reduce reliance on U. S. providers by optimizing its platform, including using a DIY content-component. This has negatively impacted revenue growth rates in 2024, and we expect revenue from this customer to decline over the next few years, regardless of whether this legislation is enforced or takes effect. It is difficult to predict whether the passed legislation will ultimately be enforced and whether any future judicial challenges brought against the Executive Order will be successful. Even though President Trump has extended the enforcement deadline for a ban on the Chinese application, there is no assurance that we will not be exposed to liability and we may be exposed to significant fines, litigation, indemnification claims, negative publicity, reputational harm, diversion of management attention, interruptions in our operations, financial loss and other similar harms by continuing to provide services to the Chinese application. In addition,** enactment and expansion of laws related to the use of artificial intelligence and machine learning in our operations and increased regulation of cloud ~~services-~~ **service** providers also could increase **the** costs of doing business, subject us to potential liability or regulatory risk and introduce other disadvantages to our business, including brand or reputational harm. Interpretations of laws or regulations that would subject us to regulatory enforcement actions, supervision or, in the alternative, require us to exit a line of business or a country, could lead to the loss of significant revenues and have a negative impact on the quality of our solutions. Engineering efforts to build new capabilities to facilitate compliance with law enforcement access requirements, content access restrictions or other regulations could require us to take on substantial expenses and divert engineering resources from other projects. These circumstances could harm our profitability. We may need to defend against patent or copyright infringement claims, which would cause us to incur substantial costs or limit our ability to use certain technologies in the future. As we expand our business and develop new technologies, products and services, we have become increasingly subject to intellectual property infringement and other claims and related litigation. We have also agreed to indemnify our customers and channel and strategic partners if our solutions infringe or misappropriate specified intellectual property rights. As a result, we have been and could again become involved in litigation or claims brought against customers or channel or strategic partners if our solutions or technology are the subject of such allegations. Any litigation or claims, whether or not valid, brought against us or pursuant to which we indemnify our customers or partners could result in substantial costs and diversion of resources and require us to do one or more of the following: cease selling, incorporating or using features, functionalities, products or services that incorporate the challenged intellectual property; pay substantial damages and incur

significant litigation expenses; obtain a license from the holder of the infringed intellectual property right, which license may not be available on reasonable terms or at all; or redesign products or services. If we are forced to take any of these actions, our business may be seriously harmed. Our business will be adversely affected if we are unable to protect our intellectual property rights from unauthorized use or infringement by third parties. We rely on a combination of patent, copyright, trademark and trade secret laws and contractual restrictions on disclosure to protect our intellectual property rights. These legal protections afford only limited protection, particularly in some regions outside the U. S. We have previously brought lawsuits against entities that we believed were infringing our intellectual property rights but have not always prevailed. Such lawsuits can be expensive and require a significant amount of attention from our management and technical personnel, and the outcomes are unpredictable. Monitoring unauthorized use of our solutions is difficult, and we cannot be certain that the steps we have taken or will take will prevent unauthorized use of our technology. Furthermore, we cannot be certain that any pending or future patent applications will be granted, that any future patent will not be challenged, invalidated or circumvented, or that rights granted under any patent that may be issued will provide competitive advantages to us. If we are unable to protect our proprietary rights from unauthorized use, the value of our intellectual property assets may be reduced. Although we have licensed from other parties proprietary technology covered by patents, we cannot be certain that any such patents will not be challenged, invalidated or circumvented. Such licenses may also be non- exclusive, meaning our competition may also be able to access such technology. Litigation may adversely impact our business. From time to time, we are or may become involved in various legal proceedings relating to matters incidental to the ordinary course of our business, including patent, commercial, product liability, breach of contract, employment, class action, whistleblower ~~and,~~ other litigation ~~and,~~ claims and governmental and other regulatory investigations and proceedings. In addition, under our charter, we could be required to indemnify and advance expenses to our directors and officers in connection with their involvement in certain actions, suits, investigations and other proceedings. Such matters can be time- consuming, divert management' s attention and resources and cause us to incur significant expenses. Furthermore, because litigation is inherently unpredictable and may not be covered by insurance, there can be no assurance that the results of any litigation matters will not have an adverse impact on our business, results of operations, financial condition or cash flows. Global climate change, other disruptions and related natural resource conservation regulations could adversely impact our business. The long- term effects of climate change on the global economy and our industry in particular remain unknown. For example, changes in weather where we operate may increase the costs of powering and cooling computer hardware we use to develop software and provide cloud ~~-based~~ services. In addition, catastrophic natural disasters, such as an earthquake, fire, flood or other act of God and any similar disruption, as well as any derivative disruption, such as those to services provided through localized physical infrastructure, including utility or telecommunication outages, or any to the continuity of our, our partners' , suppliers' and our customers' workforce, could have a material adverse impact on our business and operating results. In addition, pandemics or other public health crises, as well as any derivative disruptions such as those experienced during the COVID- 19 pandemic, in places where we operate may adversely affect our results of operations. Our global operations are dependent on our network infrastructure, technology systems and website, including the supply of servers from our third- party partners, as well as our intellectual property and personnel and any disruption to these dependencies may negatively impact our ability to respond to customers, provide services and maintain local and global business continuity. Furthermore, some of our products and business functions are hosted or carried out by third parties that may be vulnerable to these same types of disruptions, the response to or resolution of which may be beyond our control. Any disruption to our business could cause us to incur significant costs to repair damages to our facilities, equipment, infrastructure and business relationships. In addition, in response to concerns about global climate change, governments may adopt new regulations affecting the use of fossil fuels or requiring the use of alternative fuel sources which could adversely impact our business. Our deployed network of servers consumes significant energy resources, including those generated by the burning of fossil fuels. While we have invested in projects to support renewable energy development, our customers, investors and other stakeholders may require us to take more steps to demonstrate that we are taking ecologically responsible measures in operating our business. The costs and any expenses we may incur to make our network more energy- efficient and comply with any new regulations could make us less profitable in future periods. Failure to comply with applicable laws and regulations or other requirements imposed on us could lead to fines, lost revenue and damage to our reputation. Investment- Related Risks Our stock price has been, and may continue to be, volatile, and your investment could lose value. The market price of our common stock has historically been volatile. Trading prices for our common stock may continue to fluctuate in response to a number of events and factors, including the following: quarterly variations in operating results **; changes in guidance or failure to meet guidance** ; announcements by our customers related to their businesses that could be viewed as impacting their usage of our solutions; market speculation about whether we are a takeover target or considering a strategic transaction; announcements by us regarding acquisitions; announcements by competitors; activism by any single large stockholder or combination of stockholders or rumors about such activity; changes in financial estimates and recommendations by securities analysts; failure to meet the expectations of securities analysts; purchases or sales of our stock by our officers and directors; general economic conditions and other macroeconomic factors, such as inflationary pressures, foreign currency exchange rate fluctuations, energy prices, reduced consumer spending, elevated interest rates, **imposition of tariffs**, recessionary economic cycles, protracted economic slowdowns and overall market volatility; repurchases of shares of our common stock; the issuance of additional shares or securities convertible into, or exchangeable or exercisable for, shares of our common stock, including under our equity compensation plans; entry into, or termination of, relationships with material customers and partners; and performance by other companies in our industry. Furthermore, our revenue, particularly that portion attributable to usage of our solutions beyond customer commitments, can be difficult to forecast, and, as a result, our quarterly operating results can fluctuate substantially. This concern is particularly acute with respect to our media and commerce customers. In the future, our customer contracting models may change to move away from a committed revenue structure to a " pay- as- you- go " approach, which could make it

easier for customers to reduce the amount of business they do with us or leave altogether. Changes in billing models and committed revenue requirements could, therefore, create challenges with our forecasting processes. Because a significant portion of our cost structure is largely fixed in the short-term, revenue shortfalls tend to have a disproportionately negative impact on our profitability. If we announce revenue or profitability results that do not meet or exceed our guidance, **issue guidance that does not meet or exceed market expectations**, or make changes in our guidance with respect to future operating results, our stock price may decrease significantly as a result. Any of these events, as well as other circumstances discussed in these Risk Factors, may cause the price of our common stock to fall. In addition, the stock market in general, and the market prices of stock of publicly-traded technology companies in particular, have experienced significant volatility that often has been unrelated to the operating performance of affected companies. These broad stock market fluctuations may adversely affect the market price of our common stock, regardless of our operating performance. Any failure to meet our debt obligations or obtain financing would damage our business. As of the date of this report, we had total principal amount of \$ 1, 150. 0 million of convertible senior notes outstanding due in 2025, total principal amount of \$ 1, 150. 0 million of convertible senior notes outstanding due in 2027 and total principal amount of \$ 1, 265 .0 million of convertible senior notes outstanding due in 2029. We also entered into a credit facility in November 2022 that provides for an initial \$ 500. 0 million revolving credit facility, and under specified circumstances, the credit facility can be increased to up to \$ 1 billion in aggregate principal amount. As of December 31, **2023-2024**, there were no outstanding borrowings under the credit facility. Our ability to repay any amounts we borrow under our credit facility, refinance the notes, make cash payments in connection with conversions of the notes or repurchase the notes in the event of a fundamental change (as defined in the applicable indenture governing the notes) will depend on market conditions and our future performance, which is subject to economic, financial, competitive and other factors beyond our control. We also may not use the cash we have raised through future borrowing under the credit facility or the issuance of the convertible senior notes in an optimally productive and profitable manner. If we are unable to remain profitable or if we use more cash than we generate in the future, our level of indebtedness at such time could adversely affect our operations by increasing our vulnerability to adverse changes in general economic and industry conditions and by limiting or prohibiting our ability to obtain additional financing for additional capital expenditures, acquisitions and general corporate and other purposes. If we do not have sufficient cash upon conversion of the notes or to repurchase the notes following a fundamental change, we would be in default under the terms of the notes, which could seriously harm our business. Although the terms of our credit facility include certain financial ratios that potentially limit our future indebtedness, the terms of the notes do not. If we incur significantly more debt, this could intensify the risks described above. In addition, if we are unable to obtain financing to fund additional capital expenditures, acquisitions and general corporate and other purposes on reasonable terms, or at all, then our business, operations and financial condition may be harmed. Because we currently do not intend to pay dividends, stockholders will benefit from an investment in our common stock only if it appreciates in value. We currently intend to retain our future earnings, if any, for use in the operation of our business and do not expect to pay any cash dividends in the foreseeable future on our common stock. As a result, the success of an investment in our common stock will depend upon any future appreciation in its value. There is no guarantee that our common stock will appreciate in value or even maintain the price at which stockholders have purchased their shares, and our stock price has been, and may continue to be, volatile, and your investment could lose value. See the risk factor titled “ Our stock price has been, and may continue to be, volatile, and your investment could lose value ” above. Provisions of our charter, by-laws and Delaware law may have anti-takeover effects that could prevent a change in control even if the change in control would be beneficial to our stockholders. Provisions of our charter, by-laws and Delaware law could make it more difficult for a third party to control or acquire us, even if doing so would be beneficial to our stockholders. These provisions include: our board of directors having the right to elect directors to fill a vacancy created by the expansion of the board of directors or the resignation, death or removal of a director; stockholders needing to provide advance notice, additional disclosures and representations and warranties to nominate individuals for election to the board of directors or to propose matters that can be acted upon at a stockholders' meeting; and the ability of our board of directors to issue, without stockholder approval, shares of undesignated preferred stock. Further, as a Delaware corporation, we are also subject to certain Delaware anti-takeover provisions. Under Delaware law, a corporation may not engage in a business combination with any holder of 15 % or more of its capital stock unless the holder has held the stock for three years or, among other things, the board of directors has approved the transaction. Our board of directors could rely on Delaware law to prevent or delay an acquisition of us. If we fail to maintain an effective system of internal controls, we may not be able to accurately report our financial results or prevent fraud. As a result, our stockholders could lose confidence in our financial reporting, which could harm our business and the trading price of our common stock. The Sarbanes-Oxley Act requires, among other things, that we maintain effective disclosure controls and procedures and internal control over financial reporting. As previously disclosed **in our Form 10-K** for the year ended December 31, 2022, we identified a material weakness in the Company's internal control over financial reporting as of December 31, 2022 related to income taxes. Although this material weakness has been remediated, there can be no assurance that we will not identify additional material weaknesses in internal controls in the future or that the measures we may take to remediate any such future control deficiencies will be effective. We need to continue to enhance and maintain our processes and systems and adapt them to changes as our business evolves and we rearrange management responsibilities and reorganize our business. This continuous process of maintaining and adapting our internal controls and complying with Section 404 is expensive and time-consuming and requires significant management attention. Furthermore, as our business changes, including by expanding our operations in different markets, increasing reliance on channel partners and completing acquisitions, our internal controls may become more complex and we may be required to expend significantly more resources to ensure our internal controls remain effective. Failure to implement required new or improved controls, or difficulties encountered in their implementation, could harm our operating results or cause us to fail to meet our reporting obligations. If we or our independent registered public accounting firm identify additional material weaknesses, the disclosure of that fact, even if quickly remediated,

could reduce the market's confidence in our financial statements and harm our stock price. We cannot be certain that our internal control measures will provide adequate control over our financial processes and reporting and ensure compliance with Section 404. Any failure to develop or maintain effective controls, or any difficulties encountered in their implementation or improvement, could harm our operating results, may result in a restatement of our financial statements for prior periods, cause us to fail to meet our reporting obligations, and could adversely affect the results of periodic management evaluations and annual independent registered public accounting firm attestation reports regarding the effectiveness of our internal control over financial reporting that we are required to include in the periodic reports we will file with the Securities and Exchange Commission.