**Risk Factors Comparison 2025-02-20 to 2024-02-21 Form: 10-K**

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

Our business involves significant risks, some of which are described below. 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. Any of the following risks could have an adverse effect on our business, results of operations, financial condition, or prospects, and could cause the trading price of our Class A common stock to decline. Our business, results of operations, financial condition, or prospects could also be harmed by risks and uncertainties that are not presently known to us or that we currently believe are not material. In that event, the market price of our Class A common stock could decline, and you could lose part or all of your investment. Our Risk Factors are not guarantees that no such conditions exist as of the date of this report and should not be interpreted as an affirmative statement that such risks or conditions have not materialized, in whole or in part. Risks Related to Our Business and Our Industry We have a history of net losses and may not be able to achieve or sustain profitability in the future. We have incurred net losses in all periods since we began operations and we may not achieve or maintain profitability in the future. We experienced net losses of $ **78. 8 million, $** 183. 9 million, **and** $ 193. 4 ~~million, and $ 260. 3~~ million for the years ended December 31, **2024,** 2023, **and** 2022 ~~, and 2021~~ , respectively, and as of December 31, ~~2023~~ **2024** , we had an accumulated deficit of $ 1, ~~023~~ **102** . ~~8~~ **6** million. Because the markets for our products are rapidly evolving, it is difficult for us to predict our future results of operations. We expect our operating expenses to increase over the next several years as we continue to hire additional personnel, expand our operations and infrastructure both domestically and internationally, and continue to develop our products. If we fail to increase our revenue to offset the increases in our operating expenses, we may not achieve or sustain profitability in the future. We have experienced rapid revenue growth, which may not be indicative of our future performance. We have experienced rapid revenue growth in recent periods, with revenue of $ 1, **669. 6 million, $ 1,** 296. 7 million, **and** $ 975. 2 ~~million, and $ 656. 4~~ million for the years ended December 31, **2024,** 2023, **and** 2022 ~~, and 2021~~ , respectively. However, our rate of revenue growth has slowed in recent periods and may continue to slow in future periods. You should not consider our ~~recent~~ **historical** growth in revenue as indicative of our future performance. In particular, our revenue growth rates may continue to slow or decline in the future and may not be sufficient to achieve and sustain profitability, as we also expect our costs to increase in future periods. We believe that historical comparisons of our revenue may not be meaningful and should not be relied upon as an indication of future performance. Accordingly, you should not rely on our revenue and other growth for any prior quarter or year as an indication of our future revenue or revenue growth. Our historical rapid growth and fluctuations in our growth rate more recently may also make it difficult to evaluate our future prospects. Our ability to forecast our future results of operations is subject to a number of uncertainties, including our ability to effectively plan for and model future growth. 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, results of operations, and financial condition could be harmed. Adverse economic conditions, including reduced spending on products and solutions for network security, performance, and reliability, may adversely impact our revenue and profitability. Our operations and financial performance depend in part on worldwide economic conditions and the impact these conditions have on levels of spending on products and solutions for network security, performance, and reliability. Our business depends on the overall demand for these products and on the economic health and general willingness of our current and prospective customers to purchase our products. The United States, Europe, and the United Kingdom have recently experienced historically high levels of inflation. Although inflation levels have ~~begun to decrease~~ **decreased from such high levels** in the United States, the United Kingdom, and Eurozone, the U. S. Federal Reserve, the European Central Bank, and the Bank of England have **in the past** raised, and may ~~continue to~~ **in the future** raise or maintain, high interest rates and may implement fiscal policy interventions. Even if these interventions lower inflation, they may also reduce economic growth rates, create a recession, and result in other similar or unexpected effects. ~~For example, the decrease in values of government- issued securities resulting from higher interest rates may have played a significant role in the failures of Silicon Valley Bank and Signature Bank during the first quarter of 2023, the circumstances resulting in the UBS takeover of Credit Suisse during the second quarter of 2023, and generalized uncertainty confronting a number of other financial institutions.~~ Downturns in economic conditions — including inflation, rising interest rates, reductions in business confidence and activity, the curtailment of government or corporate spending, volatile financial markets, the actual or perceived failure or financial difficulties of ~~additional~~ financial institutions, ~~ongoing~~ supply chain disruptions **or increased equipment costs due to current or potential future tariffs** , and reduced demand for products and services across a variety of industries — have in the past and may in the future affect our business and our current and prospective customers and their industries adversely. For example, during an economic downturn, our current and prospective customers may suffer from reduced operating budgets. Some of our paying customers may view a subscription to our products as a discretionary purchase and may reduce their discretionary spending on our products or reduce or cut their budget to otherwise expand their subscriptions to our products. Moreover, our competitors may respond to market conditions by lowering prices and attempting to lure away our customers. Further, the sales cycle for new **and existing** customers of our technology and services could lengthen in the future as a result of challenging macroeconomic conditions, resulting in a potentially longer delay between increasing operating expenses and the generation of corresponding revenue, if any. For example, potentially as a result of these various macroeconomic impacts on our customers ~~, since the first half of 2022~~ , we periodically have experienced lengthening of the average sales cycles for certain types of customers and sales, slowdowns in our pipeline of potential new customers and in the

rate of converting sales pipeline opportunities into new sales, increases in average days sales outstanding, higher levels of churn in our paying customer base (which is when any of our paying customers cease to be a paying customer for any reason, including any pay- as- you- go customer converting to a free subscription plan), and lengthening of the timing of payment from some of our customers, all of which may have contributed to a slowdown in our revenue growth ~~over that~~ **from prior** ~~period~~ **periods** (including with respect to new customers). We may also experience increases in new and existing customers requesting concessions in terms of payment amounts and / or timing and earlier or additional termination rights in the future as the challenging macroeconomic conditions continue or worsen. We continue to monitor economic conditions to assess possible implications to our business and to take appropriate actions in an effort to mitigate the adverse consequences of uncertainty or negative trends. However, there can be no assurances that initiatives we undertake will be sufficient or successful. If there is an economic downturn that affects our current and prospective customers, or if we are unable to address and mitigate the risks associated with any of the foregoing, our business, results of operations and financial condition could be adversely affected. The ~~Hamas- Israel~~ **conflicts in the Middle East** and ~~Russia-~~Ukraine **and** ~~conflicts,~~ other areas of geopolitical tension around the world ~~,~~ or ~~the~~ **any** worsening or expansion of those conflicts or tensions **, other geopolitical events such as elections and other governmental changes** , and any related challenging macroeconomic conditions globally and in various countries in which we and our customers operate may materially adversely affect our customers, vendors, and partners, and the duration and extent to which these factors may impact our future business and operations, results of operations, financial condition, and cash flows remain uncertain. The ~~Hamas- Israel~~ **conflicts in the Middle East** and ~~Russia-~~Ukraine **and** ~~conflicts, or~~ other areas of geopolitical tension around the world ~~,~~ or any worsening or expansion of those conflicts or geopolitical tensions **, other geopolitical events such as elections and other governmental changes** , and any related challenging macroeconomic conditions globally **and in various countries in which we and our customers operate** , could decrease the spending of our existing and potential new customers, adversely affect demand for our products, cause one or more of our customers, vendors, and partners to file for bankruptcy protection or go out of business, cause one or more of our customers to fail to renew, terminate, or seek to renegotiate their contracts with us, **cause one or more of our suppliers to increase prices as a result of current or potential future tariffs or other factors,** affect the ability of our sales team to travel to potential customers, impact expected spending from existing and potential new customers, and negatively impact collections of accounts receivable, all of which could adversely affect our business, results of operations, and financial condition. Any of the negative impacts of the ~~Hamas- Israel~~ **conflicts in the Middle East** and ~~Russia-~~Ukraine **and** ~~conflicts,~~ other areas of geopolitical tension around the world ~~,~~ or any worsening **or expansion** of those conflicts or geopolitical tensions **, other geopolitical events such as elections and other governmental changes** , and any related challenging macroeconomic conditions **globally and in various countries in which we and our customers operate** , may have a material adverse effect on our business and operations, results of operations, financial condition, and cash flows. Any of these negative impacts, alone or in combination with others, also could exacerbate many of the other risk factors discussed in this Part I, Item 1A " Risk Factors " of this Annual Report on Form 10- K, including volatility in the trading prices of our Class A common stock. The full extent to which these factors will negatively affect our business and operations, results of operations, financial condition, and cash flows will depend on future developments that are highly uncertain and cannot be predicted, including the scope, severity, and duration of the ~~Hamas- Israel~~ **conflicts in the Middle East** and ~~Russia-~~Ukraine ~~conflicts~~ , other areas of geopolitical tension around the world, and any economic downturns and the actions taken by governmental authorities and other third parties in response. If we are unable to attract new paying and free customers, our future results of operations could be harmed. The success of our business principally depends on our ability to attract new paying and free customers. To do so, we must persuade decision makers at potential customers that our products offer significant advantages over those of our competitors. Other factors, many of which are out of our control, may now or in the future impact our ability to add new paying and free customers, including: • potential customers' commitments to existing equipment or vendors; • potential customers' greater familiarity and / or comfort with on- premises, appliance- based products and concerns about potential risks associated with using cloud- based solutions; • actual or perceived switching costs; • our failure to develop new products and features, and to adapt to technological developments, that our potential customers' demand, including potential large customers; • the failure of our new or existing products and features to perform in the manner demanded or expected by potential customers and our existing customers, particularly large customers; • delays in the general availability release of products and features after we have announced their development or beta availability; • our failure to generate demand for our products through effective marketing efforts related to our business and products; • our failure to obtain additional, or maintain existing, government or industry security certifications for our network and products, such as ~~the~~ Federal Risk and Authorization Management Program (FedRAMP) moderate authorization that we achieved in 2022; • negative media, industry, or financial analyst commentary regarding our products and our network and the identities and activities of some of our paying and free customers; • the adoption of new, or amendment of existing, laws, rules, or regulations that negatively impact the utility of, or increase the risk of using, cloud- based solutions generally or our network and products specifically, including changes in new or modified laws and regulations relating to privacy, data protection, and information security; • our failure to effectively recruit, expand, develop, retain, and motivate our sales and marketing personnel; • our failure to develop or expand relationships with existing channel partners or to attract new channel partners; • our failure to help or provide support to our customers, particularly large customers, in order to successfully deploy and use our products in a manner required by them, their industry, or applicable regulators; • our failure to educate our customers about our network and products; • the perceived risk, commencement, or outcome of litigation; • deteriorating general economic conditions, including inflation, rising interest rates, and the actual or perceived failure or financial difficulties of financial institutions; and • impacts of the ~~Hamas- Israel~~ **conflicts in the Middle East** and ~~Russia-~~Ukraine **and** ~~conflicts or~~ other areas of geopolitical tension around the world ~~,~~ or any worsening or expansion of those conflicts or geopolitical tensions **and impacts of geopolitical events such as elections and other governmental changes** . We believe that the importance of brand recognition for attracting new customers will increase as we

introduce new products and continue to expand into new markets. However, the promotion of our brand may require substantial expenditures. We have invested, and expect to continue to invest, substantial resources to increase our brand awareness, both generally and in specific geographies and to specific customer groups. There can be no assurance that our brand development strategies and investment of resources will enhance recognition of our brand or lead to an increased customer base. If our efforts to attract new paying customers are not successful, our revenue and rate of revenue growth may decline, we may not achieve profitability, and our future results of operations could be materially harmed. If our efforts to attract new free customers are not successful, the benefits to our network and product development cycles from our strategy of providing a free subscription plan will be diminished. Our business depends on our ability to retain and upgrade paying customers, expand the number of products we sell to paying customers, and, to a lesser extent, convert free customers to paying customers, and any decline in renewals, upgrades, expansions, or conversions could adversely affect our future results of operations. Our business is subscription- based and it is important for our business and financial results that our paying customers renew their subscriptions for our products when existing contract terms expire. Our pay- as- you- go customers pay with a credit card on a monthly or annual basis and can terminate their subscriptions, or switch to less expensive subscription plans, at will with little advance notice. Because pay- as- you- go customers that subscribe to our basic subscription plans are an important source of revenue, this ease of termination could cause our results of operations to fluctuate significantly from quarter to quarter. Our contracted customers, which consist of customers that sign up for our Enterprise plan, enter into longer term agreements typically ranging from one to three years, and they generally have no obligation to renew their subscriptions for our products after the expiration of their contractual period and are allowed to cancel their subscriptions in the case of our uncured material breach of the agreement. Some contracted customers also have agreements that allow them to terminate the agreement without cause upon little or no advance written notice, or upon our failure to meet certain service level commitments, or to obtain and maintain industry security certifications within a specified time frame. Should certain of our contracted customers, especially our large customers, terminate their agreements, or reduce their expenditures, with us, our financial condition and results of operations may materially suffer. In addition, as we continue to increase our number of large customers, and the amount of revenue we receive from large customers, this risk may increase. Due to our varied customer base and short average subscription periods, it is difficult to accurately predict our long- term customer retention rate. Our customer retention may decline or fluctuate as a result of a number of factors, including our customers' satisfaction with the security, performance, and reliability of our products and our global network, our development and general availability release of new products and features and adaptation to technological developments, our prices and subscription plans, our ability to provide adequate customer support or otherwise address customer concerns with our products, our customers' budgetary restrictions (including reductions in spending as a result of uncertain economic conditions or overall industry uncertainty), mergers, acquisitions, joint ventures, and business partnerships and relationships involving our customers, failure or bankruptcy of our customers, the perception that competitive products provide better or less expensive options, negative public perception of us or our free and paying customers, concerns about new or amended laws, rules, or regulations that increase the risk of using cloud- based solutions or our network and products specifically, and deteriorating general economic conditions. Our future financial performance also depends in part on our ability to continue to upgrade paying customers to higher- tier subscriptions, expand the number of products we sell to paying customers, and, to a lesser extent, to convert free customers into paying customers. Conversely, our paying customers may convert to lower- cost or free plans or reduce the number of products they purchase from us if they do not see the marginal value in paying for our higher- cost plans or for our specific products, or due to challenging macroeconomic conditions and / or reduced operating budgets, thereby impacting our ability to increase revenue. For example, ~~during the second and third quarters of 2022,~~ we **periodically have** experienced a higher level of churn in our paying customer base (which is when any of our paying customers cease to be a paying customer for any reason, including any pay- as- you- go customer converting to a free subscription plan). Moreover, our free customers have no obligation to transition to paying customers at any point. In order to expand our commercial relationship with our customers, existing paying and free customers must decide that the incremental cost associated with such an upgrade in their subscription plans, the purchase of additional, or the expanded use of their currently used, products is justified by the additional functionality they would gain. For example, some of our paying customers may decide that our Enterprise plan offerings do not provide sufficient incremental value to upgrade from our pay- as- you- go offering or to continue any such previously chosen upgrade. Our customers' decisions whether to upgrade their subscription, purchase additional, or expand current usage, of our products or to continue any such previously chosen upgrade or purchased products are driven by a number of factors, including customer satisfaction with the security, performance, and reliability of our network and products, customer security and networking issues and requirements, general economic conditions, and customer reaction to the price for additional products. If our efforts to expand our relationship with our existing paying and free customers are not successful, our financial condition and results of operations may materially suffer. If we are unable to effectively attract, expand, and retain sales to large customers, or we fail to mitigate the additional risks associated with serving large customers, our business, results of operation, and financial condition may suffer. Our growth strategy is dependent, in large part, upon attracting, expanding, and retaining sales to large customers. For our definition of " large customers, " see Part II, Item 7. Management' s Discussion and Analysis of Financial Condition and Results of Operations. Attracting, expanding, and retaining sales to large customers involve risks that may not be present, or that are present to a lesser extent, with sales to smaller customers, including: • competition from companies that traditionally target larger enterprises and that may have pre- existing relationships or purchase commitments from such larger enterprise customers, including companies that seek to bundle sales of their new or existing products that are competitive to our products, or that may have more experienced sales personnel or greater budgetary resources available or committed to such larger enterprise customers; • longer evaluation periods, more detailed evaluations, and more cumbersome contract negotiation and approval processes, including potential requirements for such purchasing decisions to be approved by senior executives of such companies; • increased purchasing power and leverage in

negotiating pricing terms and other contractual arrangements with us **, which may result in us being subject to additional, or greater levels of, contractual risks than our sales to smaller customers** ; • requirements for more technically complex configurations, integrations, deployments, or features; • greater customer support or assistance with migrating their systems from another vendor to our network and products; • more stringent requirements in terms of the security, performance, and reliability of our products and our network and our support and compliance obligations related to our products; • increased usage of our global network that may require us to incur greater network infrastructure expenditures; and • longer sales cycles and the associated risk that substantial time and resources may be spent on a potential customer that elects not to purchase, expand, or continue to purchase our products. Historically, the implementation period to start using, or expanding the use of, our products has been short, with most customers under our pay- as- you- go plans implementing usage of our products within a ~~matter~~ **short period** of ~~minutes~~ **time** and our sales cycle for customers under our Enterprise plan lasted less than one quarter. Since the first half of 2022, however, we have experienced periodic lengthening of our average sales cycle for our new and existing large customers, and the lengthening of our sales cycle to our large customers could continue in the future ~~to the extent that macroeconomic conditions further deteriorate~~ . In addition, as our sales force continues to target an increasing number of large customers for new and expanded product sales, these larger enterprises often undertake a more significant evaluation and negotiation processes than we have experienced in the past, which could further lengthen our sales cycle materially. In addition, our sales efforts typically involve educating our prospective large customers about the uses, benefits, and value proposition of our network and products. Our sales force develops relationships directly with our customers and our channel partners through account penetration, account coordination, sales, and overall market development. Potential large customers often view the subscription to our products, including any expansion of those subscriptions, as a significant strategic decision and, as a result, in some cases require considerable time to evaluate, test, and qualify our network and products prior to entering into or expanding a relationship with us. As a result, we spend substantial time and resources on our sales efforts without any assurance that our efforts will produce a sale. Subscriptions to our products, including expanded subscriptions, often are subject to budget constraints, multiple approvals, and unanticipated administrative, processing, and other delays. In addition, some of our subscription agreements with our large customers may have more **customer** favorable early termination rights **, less favorable limitations on liability, indemnification and other legal provisions for us** , greater usage- based pricing than is the case with our customary subscription- based agreements with our contracted customers and our pay- as- you- go customers, or generate lower margins than other contracted customers. **For example, subscription agreements with certain of our largest customers are structured on a" pool of funds" model in which the customer commits to spend at least a specified amount on our products during the subscription period. These" pool of funds" arrangements do not require the customer to subscribe for specific products or spend any specific amounts during any month, quarter or, if applicable, year of the subscription period, but the funds must be utilized during the subscription period under the terms of these subscription agreements.** As a result **of the foregoing** , it is difficult to predict whether or when a sale to a prospective large customer will be completed, how much incremental revenue or gross profit will result from such sales over the duration of the agreement, and when revenue from a subscription will be recognized or will cease. Further, our ability to improve our sales of products to large customers is dependent on us continuing to attract and retain sales personnel with experience in selling to larger enterprises. Also, because security breaches or a network outage with respect to larger, high- profile enterprises are likely to be heavily publicized, there is increased liability and reputational risks associated with serving these customers if we experience a security breach or network outage. We also believe that large customers may be more likely than our smaller customers to terminate or reduce their usage of our products in such circumstances. Once we begin selling to a large customer or expand our sales to a large customer, if we fail to retain the large customer or to retain the same amount of sales to the large customer, then the adverse impact on our result of operations and financial conditions could be significant during any specific quarter and could also result in potentially greater and unexpected variability in our results of operations and financial condition from quarter to quarter. Activities of our paying and free customers or the content of their websites or other Internet properties, as well as our response to those activities, could cause us to experience significant adverse political, business, and reputational consequences with customers, employees, suppliers, government entities, and others. Activities of our paying and free customers or the content of their websites and other Internet properties could cause us to experience significant adverse political, business, and reputational consequences with customers, employees, suppliers, government entities, and other third parties. Even if we comply with legal obligations to remove or disable customer content, we may maintain relationships with customers that others find hostile, offensive, or inappropriate. For example, we experienced significant negative publicity in connection with the use of our network by The Daily Stormer, a neo- Nazi, white supremacist website, around the time of the 2017 protests in Charlottesville, Virginia. We also received negative publicity in connection with the use of our network by 8chan, a forum website that served as inspiration for the 2019 attacks in El Paso, Texas and Christchurch, New Zealand. In 2022, we received negative publicity in connection with the use of our network by Kiwi Farms, a forum website tied to harassment campaigns and direct threats toward individuals. We are aware of some potential customers that have indicated their decision to not subscribe to our products was impacted, at least in part, by the actions or potential actions of certain of our paying and free customers. We may also experience other adverse political, business and reputational consequences with prospective and current customers, employees, suppliers, and others related to the activities of our paying and free customers, especially if such hostile, offensive, or inappropriate use is highly publicized. Conversely, actions we take in response to the activities of our paying and free customers, up to and including banning them from using our products, may harm our brand and reputation. Following the events in Charlottesville, Virginia, we terminated the account of The Daily Stormer. Similarly, following the events in El Paso, Texas, we terminated the account of 8chan, and following escalating, direct threats towards individuals in September 2022, we blocked access to Kiwi Farms content through our infrastructure. We received significant adverse feedback for these decisions from those concerned about our ability to pass judgment on our customers and the users of our network and products, or to censor them by limiting their access

to our products, and we are aware of potential customers who decided not to subscribe to our products because of this. Although offering a free plan for certain of our products is an important part of our business strategy, we may not be able to realize all of the expected benefits of this strategy and the costs and other detriments associated with our free plan could outweigh the benefits we receive from our free customers. We have historically offered a free plan for certain of our products. We believe that this strategy is valuable to us and it is an important part of our overall business strategy. However, to the extent that we do not achieve the expected benefits of this strategy, our business may be adversely affected by the costs and detriments of making certain of our products available on a free basis. While we do not receive any revenue from our free customers, we bear incremental expenses and other liabilities **and contingent liabilities, including litigation,** as a result of our free customers' continuing free use of our network and certain of our products. Adverse political, business, and reputational consequences associated with Internet properties we serve that are perceived as hostile, offensive, or inappropriate may also be disproportionately common among our free customers. The vast majority of our customers do not pay for our products. In addition, a substantial majority of our free customers historically have not converted to paying customers and we expect this will continue in the future. We face intense and increasing competition, which could adversely affect our business, financial condition, and results of operations. The markets for our network and products are intensely competitive and characterized by rapid changes in technology, customer requirements, industry standards, and frequent introductions of new, and improvements of, existing products. Our broad portfolio of products exposes us to competition from a large number of competitors in a number of different markets, including companies and their product and services offerings in, among others, virtual private networks, internal and external firewalls, web security (including web application firewalls and content filtering), distributed denial- of- service (DDoS) prevention, intrusion detection and prevention, application delivery controls, content delivery networks, domain name systems, email security vendors, advanced threat prevention, and wide area network (WAN) technology. Our competitors provide both on- premises, appliance- based solutions, and cloud- based services that have functionality similar to our network and products. We expect competition to increase as other established and emerging companies and start- ups enter the markets for products and solutions for security, performance, and reliability, in particular with respect to cloud- based solutions, as customer requirements evolve and as new products, services, and technologies **, including those that leverage artificial intelligence and machine learning,** are introduced. If we are unable to anticipate or effectively react to these competitive challenges, our competitive position could weaken, and we could experience a decline in revenue or our growth rate that could materially and adversely affect our business and results of operations. Our potential competitors include large companies with substantial infrastructure, such as global telecommunications services provider partners and public cloud providers. These companies could choose to enter the markets for products and solutions for security, performance, and reliability, including by acquiring existing companies, developing their own internal solutions, or establishing cooperative relationships with businesses that may allow them to offer more comprehensive solutions or to offer solutions for lower prices or to adapt more quickly than us to new technologies and customer needs. As our business continues to grow and we increase our market share for various products and services, these larger companies may increase their focus on us as a competitor and the actions they undertake to compete with our business and products. Additionally, if an increasing portion of web content is housed on another company' s network or portions of the Internet are otherwise privatized, it could reduce the demand for our products and increase competitive pressure on us. These competitive pressures in our markets or our failure to compete effectively may result in price reductions, fewer subscriptions, reduced revenue and gross margin, increased net losses, and loss of market share. Our current competitors include a number of different types of companies, including: • on- premises network hardware vendors; • point solution vendors, which provide cloud- based products and services to address a single use case or challenge, in various categories including cloud security vendors, content delivery network (CDN) vendors, domain name system (DNS) services vendors, email security vendors, and cloud SD- WAN vendors; and • traditional public cloud vendors. Many of our existing and potential competitors have or could have substantial competitive advantages including, among others: • greater name recognition; • longer operating histories; • larger customer bases; • larger sales and marketing budgets and capital resources; • broader distribution and established relationships with channel partners and customers; • greater customer support resources; • greater resources to make acquisitions and enter into strategic partnerships; • lower labor and research and development costs; • more mature products and services developed for large customers; • larger and more mature intellectual property rights portfolios; • control of significant technologies, standards, or networks, including operating systems, with which our products must interoperate; • higher or more difficult to obtain security certifications than we possess; and • substantially greater financial, technical, and other resources. In addition, some of our larger competitors have substantially broader and more diverse product and services offerings, which may allow them to leverage existing commercial relationships, incorporate functionality into existing products, sell products and services with which we compete at zero or negative margins, offer fee waivers and reductions or other economic and non- economic concessions, bundle products and solutions, maintain closed technology platforms, or render our products unable to interoperate with such platforms. If they were to engage in predatory competitive practices, it could harm our existing product offerings or prevent us from creating viable products in other segments of the markets in which we participate. If our competitors are able to exploit their advantages or are able to persuade our customers or potential customers that their products are superior to ours, we may not be able to compete effectively and our business, financial condition, and results of operations may be materially affected. If we do not effectively attract, train, and retain our sales force to be able to sell our existing and new products and product features, we may be unable to add new contracted customers, or increase sales to our existing customers and our business would be adversely affected. A substantial majority of our revenue in the year ended December 31, ~~2023~~ **2024** was from contracted customers that were acquired through our inside and field sales teams, and we expect our sales teams to continue generating the majority of our revenue for the foreseeable future. As a result, our financial condition and results of operations are dependent to a significant degree on our ability to effectively attract, train, and retain qualified sales personnel, including senior sales leaders, and the ability of our dedicated sales

personnel to acquire new contracted customers and expand our relationships with our existing contracted customers. Our sales representatives typically engage in direct interaction with our prospective contracted customers. Increasing our customer base and achieving broader market acceptance of our network and products will depend, to a significant extent, on our ability to expand and further invest in our sales and marketing operations and activities. There is significant competition for sales personnel with the advanced sales skills and technical knowledge we need. We believe that selling subscriptions to our products requires particularly talented sales personnel that understand a very wide array of highly technical topics, including significant portions of global networking, Internet, enterprise and identity security, and application development for both on- premises and cloud requirements. In addition, as we continue to develop and sell newer types of products and product features, such as our ~~Cloudflare One~~ suite of **Zero Trust and network services** solutions and our developer suite of products, we will need our sales personnel to be proficient in selling both these newer products and features and our overall broader suite of products to our existing and potential customers. Changes in the senior leadership of our sales team, such as the departure of our former President of Revenue and the hiring of our new President of Revenue in February 2024 **and subsequent changes to a number of the other senior leadership positions within our sales team** , ~~also~~ could negatively impact our ability to retain current members of our sales team. If we are unable to effectively attract, train, and retain qualified sales personnel, particularly as our lines of products and product features expand, our business, results of operations, and financial condition will be adversely impacted. Our ability to achieve significant growth in revenue in the future also will depend, in large part, on our success in recruiting, training, and retaining sufficient numbers of these talented sales personnel in both the United States and international markets. In addition, our ability to effectively recruit and retain qualified sales personnel outside the United States is reduced if we do not have a local subsidiary and office in that country or, if we do have such a subsidiary and office, we will experience increased costs in operating in that country. Furthermore, hiring sales personnel in new countries, or expanding our existing presence in the countries in which we currently operate, requires upfront and ongoing expenditures that we may not recover if the sales personnel fail to achieve full productivity or that may be recovered on a more delayed basis than expected. As we continue to focus on revenue growth, we are seeking to increase our rate of hiring sales personnel and any delays in making these incremental sales hires could have an adverse impact on our ability to increase revenue, particularly with respect to our sales to contracted customers. In addition, if we fail to effectively train and integrate new hires, it could negatively impact the existing sales and marketing personnel and their productivity, relationships with our customers, our ability to generate a pipeline of new customers, and our ability to increase revenue. New sales hires require significant training and may take significant time before they achieve full productivity. As a result, our new sales hires and planned sales hires may not become as productive as we would like or as quickly as we expect, and we may be unable to hire or retain sufficient numbers of qualified individuals. In addition, due to our rapid growth, a large percentage of our sales team is new to our company and inexperienced in selling subscriptions to our products, and therefore these personnel may be less effective than our more seasoned employees. For example, **since** ~~beginning in~~ late 2022 ~~and continuing through the end of the first quarter of 2023~~ , we **periodically have** experienced a reduction in average productivity among our sales personnel, which we believe was due in part to new sales hires not becoming as productive as we expected and exacerbated by worsening **or uncertain** macroeconomic conditions. While we continue to address productivity and focus on hiring, training, and retaining successful sales personnel, these efforts may take longer than anticipated, which may negatively impact our ability to achieve our targeted revenue growth. In addition, experienced sales personnel are particularly sought after in our industry and we believe our company' s recent growth and increased profile may result in increased efforts by other companies to hire our sales personnel. As a result, we may have to expend significant resources to retain our most productive sales employees. Even with considerable effort, we may be unsuccessful at retaining our experienced sales employees, which would adversely impact our business, results of operations, and financial condition. We cannot predict whether, or when or to what extent, our sales will increase as we expand our sales force or how long it will take for sales personnel to become productive. If we are unable to hire, train, and retain a sufficient number of effective sales personnel, or the sales personnel we hire are not successful in obtaining new customers or increasing sales to our existing customer base, our business and future growth prospects will be materially and adversely affected. If we fail to effectively manage our growth, we may be unable to execute our business plan, maintain high- quality levels of customer support, ensure the reliability and security of our network, adequately address competitive challenges, or maintain our corporate culture, and our business, financial condition, and results of operations would be harmed. We have experienced, and may in the future experience, periods of rapid growth. For example, our headcount grew from ~~2, 439 employees as of December 31, 2021, to~~ 3, 217 employees as of December 31, 2022, to 3, 682 employees as of December 31, 2023 **, to 4, 263 employees as of December 31, 2024** . We also have expanded the locations where we have employees to a number of new locations around the world during the past several years. The number of customers, users, and requests on our network also has increased rapidly in recent years. While we expect to continue to expand our operations, network, and products significantly in the future, both domestically and internationally, our growth may not be sustainable. Our growth has placed, and future growth will continue to place, a significant strain on our management and our administrative, operational, and financial infrastructure. Our success will depend in part on our ability to manage this growth effectively, which will require that we continue to improve our administrative, operational, financial, and management systems and controls by, among other things: • effectively attracting, training, and integrating a large number of new employees, particularly members of our sales, marketing, engineering, and management teams; • effectively managing a rapidly increasing number of employees in a growing number of countries around the world, particularly in circumstances when employees are working completely remotely; • ensuring the integrity and security of our network and IT infrastructure throughout the world; • maintaining our corporate culture, which we believe fosters innovation, teamwork, and an emphasis on customer- focused results and contributes to our cost- effective business model; • successfully acquiring and integrating companies and assets to improve, expand, and diversify our business and products through strategic acquisitions, investments, and partnerships; • further improving our key business applications, processes, and IT

infrastructure, including our network co- location facilities, to support our current and anticipated business needs; • enhancing our information and communication systems to ensure that our employees and offices around the world are well coordinated and can effectively communicate with each other and our growing base of channel partners, customers, and users; • maintaining high levels of customer support; and • appropriately documenting and testing our IT systems and business processes. Managing our growth will require significant capital expenditures and allocation of valuable management and employee resources. If we fail to manage our expected growth, the uninterrupted and secure operation of our network and products and key business systems, our corporate culture, our compliance with the rules and regulations applicable to our operations, the quality of our products, and our ability to compete could suffer. Any failure to preserve our culture also could further harm our ability to retain and recruit personnel, innovate and create new products, operate effectively, and execute on our business strategy. Our quarterly results may fluctuate significantly and may not fully reflect the underlying performance of our business. Our quarterly results of operations, including our revenue, gross margin, operating margin, profitability, cash flow from operations, deferred revenue, and backlog, may vary significantly in the future 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 quarterly 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. Fluctuation in quarterly results may negatively impact the trading price of our Class A common stock. Factors that may cause fluctuations in our quarterly results of operations include: • our ability to attract new paying customers, especially large customers, and, to a lesser extent, convert free customers to paying customers; • our ability to retain and upgrade paying customers and expand the number of products sold to paying customers, especially our large customers; • the timing of expenses and recognition of revenue; • the amount and timing of operating expenses related to the maintenance and expansion of our business, operations, and infrastructure, as well as entry into operating and capital leases and co- location, interconnection, and similar agreements related to the expansion of our network; • the timing of expenses related to acquisitions; • any large indemnification payments to our customers or other third parties; • changes in our pricing policies or those of our competitors; • the timing and success of new products, product features and service introductions by us or our competitors; • network outages or actual or perceived security breaches or incidents; • our involvement in litigation or regulatory enforcement efforts, or the threat thereof; • changes in the competitive dynamics of our industry, including consolidation among competitors and the emergence of new competitors; • increases in length of the sales cycle for our contracted customers, particularly as the relative proportion of our revenue from large customers increases and as the sizes of our large customers increase; • changes in laws and regulations that impact our business; and • general political, regulatory, economic, market, and social conditions, including inflation, rising interest rates, actual or perceived failure or financial difficulties of financial institutions, other adverse changes in global and regional macroeconomic conditions, and other impacts of the ~~Hamas- Israel~~ **conflicts in the Middle East** and ~~Russia–~~Ukraine ~~conflicts~~, or other areas of geopolitical tension around the world, or any worsening **or expansion** of those conflicts or geopolitical tensions. We rely on our co- founders and other key technical, sales, and management personnel to grow our business, and the loss of one or more key employees or the inability to successfully attract, integrate, and retain qualified senior management and other personnel, or the failure of new members of our management team to successfully lead and scale our business, could harm our business. Our future success is substantially dependent on our ability to attract, integrate, retain, and motivate the members of our management team and other key employees throughout our organization. In particular, we are highly dependent on the services of our co- founders, Matthew Prince, our Chief Executive Officer, and Michelle Zatlyn, our President ~~and Chief Operating Officer~~. We rely on our leadership team in the areas of operations, security, marketing, sales, support, research and development, and general and administrative functions, and on individual contributors on our research and development team. Although we have entered into employment offer letters with our key personnel, these agreements have no specific duration and constitute at- will employment. We also do not maintain key person life insurance policies on any of our employees. From time to time, there may be changes in our management team as a result of the hiring, departure or realignment of our senior management and other key personnel, and such changes may impact our business. Additionally, as our business grows in scale and complexity, other changes to our management team may be necessary. For example, ~~during 2023,~~ we **have** hired several new members of our senior management team **in the past year**, including our ~~Senior Vice~~ President **of Revenue**, **our Chief Strategy Officer, and our President of Product and** Engineering ~~; Senior Vice President, Chief Security Officer; and Senior Vice President, Chief People Officer, and our Chief Product Officer left the Company. In addition, in February 2024, our former President of Revenue departed and we hired our new President of Revenue~~. Any significant leadership change or senior management transition, such as these, involves inherent risks and any failure to ensure timely and suitable replacements and smooth transitions could hinder our strategic planning, business execution, and future performance. In particular, these or any future leadership transitions may result in **, and in some cases have resulted in,** a loss of personnel with deep institutional or technical knowledge and changes in business strategy or objectives and ~~have the potential to disrupt~~ **disruptions in** our operations and relationships with existing employees and customers due to added costs, operational inefficiencies, changes in strategy, decreased employee morale and productivity, and increased turnover. We must successfully integrate our new leadership team members within our organization to achieve our operating objectives. If we lose one or more of our senior management or other key employees and are unable to find adequate replacements, or if we fail to successfully attract, integrate, retain and motivate members of our senior management team and key employees, our business could be harmed. To execute our growth plan, we must also attract and retain large numbers of highly qualified personnel in a number of job markets globally. In particular, it is critical for us to attract and retain sales and engineering talent in our fast growing industry. Competition for these personnel in the San Francisco Bay Area, where our headquarters is located, and in Lisbon, London, Singapore, **and** Austin, Texas, ~~and~~ **as well as** other locations where we employ personnel, is intense, especially for experienced sales professionals and for engineers experienced in designing and developing cloud applications. We have from time to time experienced, and we may continue to experience, difficulty in hiring and

retaining employees with appropriate qualifications or level of experience. For example, we have experienced, and may continue to experience, difficulty recruiting, hiring, and retaining sales personnel with the appropriate level of experience and knowledge necessary to effectively sell our products to large customers. Additionally, in recent years, recruiting, hiring, and retaining employees with expertise in the cybersecurity industry has become increasingly difficult as the demand for cybersecurity professionals has increased as a result of high- profile cybersecurity attacks on global corporations and governments. Many of the companies with which we compete for experienced personnel have greater resources than we have and may provide higher levels of compensation or more attractive benefits. We may need to increase our existing compensation levels in response to competition, rising inflation, or labor shortages, which may increase our operating costs and reduce our margins. In addition, job candidates and existing employees often consider the value of the equity awards they receive in connection with their employment. Volatility or lack of performance in our stock price has in the past, and may in the future, affect our ability to attract and retain our key employees or require us to increase the number of shares that we include in employee equity awards, which has and may continue to affect our outstanding share count, cause dilution to existing shareholders, and increase our stock- based compensation expense. In addition, upon vesting of equity awards, many of our employees have acquired or may soon acquire a substantial amount of personal wealth. This may make it more difficult for us to retain and motivate these employees, and this wealth could affect their decision about whether or not they continue to work for us. Any failure to successfully attract, integrate, or retain qualified personnel to fulfill our current or future needs could materially and adversely affect our business, results of operations, and financial condition. We believe our long- term value as a company will be greater if we focus on growth, which may negatively impact our profitability. A significant part of our business strategy is to focus on long- term growth and to reinvest our cash flow from operations into our business, including the expansion of our global network, the development of new products and features, the expansion of our global workforce, and the potential acquisition of complementary businesses. ~~For example, in the year ended December 31, 2023, we increased our operating expenses to $ 1, 175. 2 million as compared to $ 943. 8 million and $ 637. 0 million in the years ended December 31, 2022 and 2021, respectively. In the year ended December 31, 2023 we decreased our net loss to $ 183. 9 million as compared to $ 193. 4 million and $ 260. 3 million in the years ended December 31, 2022 and 2021, respectively.~~ As a result, ~~we may continue to operate at a loss or~~ our profitability may be lower than it would be if our strategy were to maximize short- term profitability. Significant expenditures on sales and marketing efforts, and expenditures on growing our network and expanding our research and development and portfolio of products, each of which we intend to continue to invest in, may not ultimately grow our business or cause long- term profitability. If we are ultimately unable to achieve or improve profitability at the level or during the time frame anticipated by industry or financial analysts and our stockholders, our stock price may decline. If we are not able to maintain and promote our brand, our business and results of operations may be adversely affected. We believe that maintaining and enhancing our reputation as a provider of products with the highest levels of security, performance, and reliability is critical to our relationship with our existing customers and our ability to attract new customers. The successful promotion of our brand will depend on a number of factors, including the reliability of our network on which we provide our products and the record of security, performance, and reliability of our products; the timing of releases of our products and related features after the public announcement of such expected products and features; our marketing efforts; our ability to continue to develop high- quality features and products for our network; and our ability to successfully differentiate our products from competitive products and services. Our brand promotion activities may not be successful or yield increased revenue. Independent industry and financial analysts often provide reviews of our products, as well as those of our competitors. Perception of our offerings in the marketplace may be significantly influenced by these expert reviews. In addition, the difficulty or inability of us to periodically provide certain types of financial information about our business and products requested by industry analysts could adversely impact these analysts' reviews of our products. If reviews of our products are negative, or less positive than those of our competitors', our brand may be adversely affected. The performance of our channel partners also may affect our brand and reputation, particularly if customers do not have a positive experience with our channel partners. The promotion of our brand requires us to make substantial expenditures, and we anticipate that the expenditures will increase as our markets become more competitive and we expand into new markets and products. Expenditures intended to maintain and enhance our brand may not be cost- effective or effective at all. If we do not successfully maintain and enhance our brand, we may have reduced pricing power relative to our competitors, we could lose customers, or we could fail to attract potential new customers or expand sales to our existing customers, all of which could materially and adversely affect our business, results of operations, and financial condition. We have limited experience with some of our pricing models, particularly for our newer products and solutions as well as bundled sales of our products and solutions, and we may not accurately predict the long- term rate of paying customer adoption or renewal, or the impact these will have on our revenue or results of operations. We generate revenue primarily from subscriptions to our products. We offer subscription plans that provide varying degrees of functionality **and usage**, and also offer separate subscriptions to various add- on products and network functionality **and usage**. We have limited experience with respect to determining the optimal prices and pricing models for some of our newer subscription plans and products, as well as our bundled sales of products and solutions and our ~~recently- introduced~~ professional services to assist some of our large customers in their migration from existing vendors and otherwise with the configuration and use of our products. As the markets for our products mature, as we enter into newer product markets for our business, as we shift the way in which we sell our products and solutions, or as new competitors introduce new products or services that compete with ours, we may be unable to attract new customers or retain existing customers at the same price or based on the same pricing model as we have used historically. Moreover, our increasing focus on larger customers may lead to greater price concessions in the future or have a more significant impact period to period on our revenue and results of operations ~~. As a result, in the future we may be required to reduce our prices, which could adversely affect our revenue, gross margin, profitability, financial condition, and cash flow~~. We also have limited experience in determining which products and functionality to offer as part of our subscription plans,

which to offer as add- on products, and which related products to sell in bundles. Our limited experience in determining the optimal manner in which to bundle and price our various products and functionalities could reduce our ability to capture the value delivered by our offerings, which could adversely impact our business, results of operations, and financial condition. Our growth depends, in part, on the success of our strategic relationships with third parties, and if we fail to continue to expand, grow, and retain these relationships then our business, results of operations, and financial condition may be adversely impacted. To grow our business, we anticipate that we will continue to depend on relationships with third parties, such as value- added channel partners, referral partners, systems integrators, global platform providers, telecommunications companies, and managed security service providers. Developing, expanding, and retaining these strategic relationships has played, and will continue to play, an increasingly greater role in our sales efforts, especially with our large customers. However, identifying these types of strategic partners, negotiating and documenting our business and contractual relationships with them, maintaining application programming interfaces (APIs) that some of our strategic partners use to interact with our business, and monitoring the actions of our channel partners and their relationships with our end customers, each require significant time and resources **and could negatively impact the timing of sales that involve our partners** . While in some cases our contractual arrangements with our strategic partners have terms of one year or longer, in many cases these arrangements are short- term in nature and can be terminated on 90 days advance notice. Our competitors also may be effective in providing incentives to third parties to favor their products or services over subscriptions to our products. In addition, acquisitions of such strategic partners by our competitors could result in a decrease in the number of our current and potential customers, as these partners may no longer facilitate the adoption of our applications by potential customers or may seek to terminate their relationships with us. Further, some of our partners are or may become competitive with certain of our products and may elect to no longer integrate with our network and products. If we are unsuccessful in establishing, expanding, or maintaining our relationships with these third parties, our ability to compete in the marketplace or to grow our revenue could be impaired, and our business, results of operations, and financial condition may suffer. Even if we are successful, we cannot assure you that these relationships will result in increased customer usage of our products by, or increased revenue from, our paying customers and large customers. Our ability to maintain customer satisfaction depends in part on the quality of our customer support. Failure to maintain high- quality customer support could have an adverse effect on our business, results of operation, and financial condition. We believe that the successful adoption and usage of our network and products requires a high level of support and engagement for many of our customers, particularly our large customers. In order to deliver appropriate customer support and engagement, we must successfully assist our customers in deploying and continuing to use our network and products, migrating from their existing vendors, resolving performance issues **and billing inquiries** , addressing interoperability challenges with the customers' existing IT infrastructure, and responding to security threats and cyber attacks and performance and reliability problems that may arise from time to time. The IT architecture of our contracted customers, particularly the larger organizations, is very complex and may require high levels of focused technical support to effectively migrate from each customer' s existing vendors and to utilize our network and products. Because our network and products are designed to be highly configurable and to rapidly implement customers' reconfigurations, customer errors in configuring our network and products can result in significant disruption to our customers. Our support organization faces additional challenges associated with large customers in highly regulated industries, as well as our international operations, including those associated with delivering support, training, and documentation in languages other than English. Increased demand for customer support, without corresponding increases in revenue, could increase our costs and adversely affect our business, results of operations, and financial condition. In addition, we ~~have recently begun providing~~ **provide** professional services to assist some of our large customers in their migration from existing vendors and otherwise with the configuration and use of our products. We do not have significant experience in providing professional services or determining the pricing for such services, and our failure to provide such services effectively or at pricing that appropriately reflects our costs of providing such services could negatively impact our customer satisfaction and retention and our results of operations. We also rely on channel partners in order to provide migration assistance and frontline support to some of our customers, including in regions where we do not have a significant physical presence or the customers primarily speak languages other than English. If our channel partners do not provide assistance and support to the satisfaction of our customers, we may lose these customers, such customers may reduce their usage of our products, or we may be required to hire additional personnel and to invest in additional resources in order to provide an adequate level of assistance and support, generally at a higher cost than that associated with our channel partners. There can be no assurance that we will be able to hire sufficient support personnel as and when needed, particularly if our sales exceed our internal forecasts. To the extent that we are unsuccessful in hiring, training, and retaining adequate support resources, our ability to provide high- quality and timely support to our customers will be negatively impacted, and our customers' satisfaction with our network and products could be adversely affected. Any failure to maintain high- quality customer support, or a market perception that we do not maintain high- quality customer support, could adversely affect our reputation, business, results of operations, and financial condition, particularly with respect to our large customers. Our business depends, in part, on sales to the United States and foreign government organizations, which are subject to a number of challenges and risks. We derive a portion of our revenue from contracts with government organizations, and we believe the success and growth of our business will in part depend on adding additional public sector customers. However, demand from government organizations is often unpredictable, and we cannot assure you that we will be able to maintain or grow our revenue from the public sector. Sales to government entities are subject to substantial additional risks that are not present in sales to other customers, including: • selling to government agencies can be more competitive, expensive, and time- consuming than sales to other customers, often requiring significant upfront time and expense without any assurance that such efforts will generate a sale; • increasing numbers of U. S., European, **Asian,** or other government certification and audit requirements potentially applicable to our network, including FedRAMP in the United States, are often difficult and costly to obtain and maintain, and failure to do so will restrict our ability to sell to government

customers in the applicable jurisdictions; • government demand, payment for, and continued usage of, our products may be impacted by public sector budgetary cycles, funding authorizations, or government shutdowns; • governments routinely investigate and audit government contractors' administrative processes and any unfavorable audit could result in fines, civil or criminal liability, further investigations, damage to our reputation, and debarment **, suspension, or ineligibility** from **some or all** further **business with the applicable** government ~~business~~ **and its related agencies and departments** ; • governments often require contract terms that differ from our standard customer arrangements, including terms that can lead to those customers obtaining broader rights in our products than would be expected under a standard commercial contract and terms that can allow for early termination **or subject us to more onerous obligations and requirements than our standard customer arrangements, such as supply chain restrictions, restrictions on employees' ability to manage their accounts, and additional reporting obligations** ; • governments may require us to partner with companies based in the governments' jurisdictions in order for us to sell any of our products to those governments, which could result in a loss of revenue we otherwise would receive for such sales; ~~and~~ • governments may demand better pricing terms and public disclosure of such pricing terms, which may harm our ability to negotiate pricing terms with our non- government customers **; and • governments may demand the use of local data centers, labor, or subcontractors which may require significant upfront increase in headcount and other expenses** . In addition, we must comply with laws and regulations relating to the formation, administration, and performance of contracts with the public sector, including U. S. federal, state, and local governmental organizations, as well as foreign governmental organizations, which affect how we and our channel partners do business with governmental agencies. Selling our products to the U. S. government, whether directly or through channel partners, also subjects us to certain regulatory and contractual requirements, including expanded compliance obligations under the Federal Acquisition Regulations (FARs). Failure to comply with these laws, regulations, and requirements by either us or our channel partners could subject us to investigations, fines, and other penalties, which could have an adverse effect on our business, results of operations, and financial condition. For example, the U. S. Department of Justice (DOJ) and the General Services Administration (GSA) have in the past pursued claims against and financial settlements with vendors under the False Claims Act and other statutes related to misrepresenting cybersecurity practices or protocols, pricing and discount practices and compliance with certain provisions of GSA contracts. The DOJ and GSA continue to actively pursue such claims. Violations of certain regulatory and contractual requirements could also result in us being suspended or debarred from future government contracting. Any of these outcomes could have a material adverse effect on our revenue, results of operations, and financial condition. Any inability to address these risks and challenges could reduce the commercial benefit to us or otherwise preclude us from selling subscriptions to our products to government organizations. We rely on third- party software for certain essential financial and operational services, and a failure or disruption in these services could materially and adversely affect our ability to manage our business effectively. We rely on third- party software to provide many essential financial and operational services to support our business ~~, including NetSuite, Salesforce, Atlassian, Stripe, and Workday among others~~ . ~~Many~~ **Some** of these vendors are less established and have shorter operating histories than traditional software vendors. Moreover, these vendors provide their services to us via a cloud- based model instead of software that is installed on our premises. As a result, we depend upon these vendors to provide us with services that are always available and are free of errors or defects that could cause disruptions in our business processes. Any failure by these vendors to do so, or any disruption in our ability to access the Internet, would materially and adversely affect our ability to manage our operations. Our business is exposed to risks associated with credit card and other online payment processing methods. Many of our customers pay for our service using a variety of different payment methods, including credit and debit cards, prepaid cards, direct debit, and online payment applications and wallets. We rely on internal systems as well as those of third parties to process payments. Acceptance and processing of these payment methods are subject to certain rules and regulations and require payment of interchange and other fees. To the extent there are increases in payment processing fees, material changes in the payment ecosystem, such as large re- issuances of payment cards, delays in receiving payments from payment processors, changes to rules or regulations concerning payment processing, loss of payment partners, and / or disruptions or failures in our payment processing systems or payment products, including products we use to update payment information, our revenue, operating expenses, and results of operation could be adversely impacted. In addition, from time to time, we encounter fraudulent use of payment methods, which could impact our results of operations and if not adequately controlled and managed could create negative consumer perceptions of our service. If we are unable to maintain our chargeback rate at acceptable levels, card networks may impose fines and our card approval rate may be impacted. If we fail to comply with the rules or requirements applicable to processing payments, or if our data security systems are breached, compromised, or otherwise unable to detect or prevent fraudulent activity, we may be liable for card issuing banks' costs, subject to fines and higher transaction fees, and lose our ability to accept certain payments from our customers. The termination of our ability to process payments using any major payment method our business, results of operations, and financial condition could be harmed. Because we recognize revenue from subscriptions for our products over the term of the subscription, downturns or upturns in new business may not be immediately reflected in our results of operations and may be difficult to discern. We generally recognize revenue from customers ratably over the term of their subscription, which in the case of our contracted customers typically range from one to three years and in the case of our pay- as- you- go customers is typically monthly. **In addition, our subscription agreements with certain of our largest customers are structured on a" pool of funds" model in which the customer commits to spend at least a specified amount on our products during the subscription period. These " pool of funds " arrangements do not require the customer to subscribe for specific products or spend any specific amounts during any month, quarter or, if applicable, year of the subscription period, but the funds must be utilized during the subscription period under the terms of these subscription agreements.** Consequently, any increase or decline in new sales or renewals to these customers in any one period may not be immediately reflected in our revenue for that period. Any such change, however, may affect our revenue in future periods. Accordingly, the effect of

downturns or upturns in new sales and potential changes in our rate of renewals may not be fully reflected in our results of operations until future periods. We may also be unable to reduce our cost structure in line with a significant deterioration in sales or renewals. Our subscription model also makes it difficult for us to rapidly increase our revenue through additional sales in any period, as **it is difficult to predict when** revenue from new customers ~~must~~ **will** be recognized over the applicable subscription term. By contrast, a significant majority of our costs are expensed as incurred, which occurs as soon as a customer starts using our network and products. As a result, an increase in customers could result in our recognition of more costs than revenue in the earlier portion of the subscription term. We may not attain sufficient revenue to maintain positive cash flow from operations or achieve profitability in any given period. If our estimates, assumptions, or judgments relating to our critical accounting policies prove to be incorrect or financial reporting standards or interpretations change, our results of operations could be adversely affected. The preparation of financial statements in conformity with generally accepted accounting principles in the United States (U. S. GAAP) requires our management to make estimates, assumptions, and judgments that affect the amounts reported and disclosed in our consolidated financial statements and accompanying notes. We base our estimates and assumptions on historical experience and on various other assumptions that we believe to be reasonable under the circumstances. The results of these estimates and assumptions form the basis for making judgments about the carrying values of assets, liabilities, and equity, and the amount of revenue and expenses that are not readily apparent from other sources. Significant estimates, assumptions, and judgments used in preparing our consolidated financial statements include those related to allowance for doubtful accounts, deferred contract acquisitions costs, the period of benefit generated from our deferred contract acquisition costs, the capitalization and estimated useful life of internal- use software, valuation of acquired intangible assets, the assessment of recoverability of intangible assets and their estimated useful lives, useful lives of property and equipment, the determination of the incremental borrowing rate used for operating lease liabilities, the valuation and recognition of stock- based compensation expense, uncertain tax positions, and the recognition and measurement of current and deferred income tax assets and liabilities. Due to geopolitical and macroeconomic uncertainties, including but not limited to the ongoing conflicts **in the Middle East** ~~between Hamas and Israel and between Russia~~ and Ukraine, and other areas of geopolitical tension around the world, inflationary pressures **, threats of tariffs and other impediments to cross- border trade** , and changes in interest rates, there is ongoing uncertainty ~~and significant disruption~~ in the global economy and financial markets. We are not aware of any specific event or circumstance that would require an update to our estimates or assumptions or a revision of the carrying value of assets or liabilities as of February ~~21~~ **20** , ~~2024~~ **2025** , the date of issuance of this Annual Report on Form 10- K. These estimates and assumptions may change in the future, however, as new events occur and additional information is obtained. Our results of operations may be adversely affected if our assumptions change or if actual circumstances differ from those in our assumptions, which could cause our results of operations to fall below the expectations of industry or financial analysts and investors, resulting in a decline in the trading price of our Class A common stock. Additionally, we regularly monitor our compliance with applicable financial reporting standards and review new pronouncements and drafts thereof that are relevant to us. As a result of new standards, or changes to existing standards, and changes in their interpretation, we might be required to change our accounting policies, alter our operational policies and implement new or enhance existing systems so that they reflect new or amended financial reporting standards, or we may be required to restate our published financial statements. Such changes to existing standards or changes in their interpretation may have an adverse effect on our reputation, business, financial condition, and profit and loss, or cause an adverse deviation from our revenue and operating profit and loss target, which may negatively impact our results of operations. Future acquisitions, strategic investments, partnerships, or alliances could be difficult to identify and integrate, divert the attention of key management personnel, disrupt our business, dilute stockholder value, and adversely affect our results of operations, financial condition, and prospects. Part of our business strategy is to make acquisitions of other companies, products, and technologies. To date, our acquisitions typically have consisted of companies that have developed technology that is complementary to our business but have small numbers of employees and little, if any, customers and revenue. We have limited experience in making acquisitions and integrating acquired businesses into our company, particularly companies with large numbers of employees and customers. However, we expect the number of acquisitions that we undertake to increase and some of the businesses we acquire will have significantly larger numbers of employees and customers and more global operations ~~. For example, in April 2022, we acquired Area 1 Security, Inc., a company that has developed cloud- native email security technology and has a significantly greater number of employees and customers~~ than our ~~prior~~ **historical** acquisitions. In addition, 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. If we identify companies that we would like to buy, we may also face antitrust, competition, and other regulatory scrutiny that may limit our ability to complete such acquisitions. 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 customers, 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 integrate and retain the people, technologies or customers associated with those acquisitions, into our company, the results of operations of the combined company could be adversely affected. Any integration process in connection with an acquisition will require significant time and resources, require significant attention from management, and disrupt the ordinary functioning of our business, and we may not be able to manage the process successfully, which could adversely affect our business, results of operations, and financial condition. We also frequently provide significant incentives for key employees of acquired companies to remain as our employees after the completion of the acquisition in order to facilitate integration and allow us to achieve the benefits we expect from the acquisition, but these incentives may not prove to be successful in retaining those new key employees. 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. In order to expand our network and product offerings, we also may enter into relationships with other businesses, which could involve joint

ventures, preferred or exclusive licenses, additional channels of distribution, or investments in other companies. Negotiating these transactions can be time- consuming, difficult, and costly, and our ability to close these transactions may be subject to third- party approvals, such as government regulatory approvals, which are beyond our control. Consequently, we cannot assure you that these transactions, once undertaken and announced, will close or will lead to commercial benefit for us. In connection with the foregoing strategic transactions, we may: • issue additional equity securities that would dilute our stockholders; • use cash that we may need in the future to operate our business; • incur debt on terms unfavorable to us or that we are unable to repay; • incur large charges or substantial actual or contingent liabilities associated with acquired businesses; • encounter difficulties integrating diverse business cultures and retaining employees and customers of acquired companies; and • become subject to adverse tax consequences, substantial depreciation, or deferred compensation charges. These challenges related to acquisitions or other strategic transactions could adversely affect our business, results of operations, financial condition, and prospects. Certain of our key business metrics could prove to be inaccurate, and any real or perceived inaccuracies may harm our reputation and negatively affect our business. We rely on assumptions and estimates to calculate certain of our key business metrics, such as dollar- based net retention rate. We regularly review and may adjust our processes for calculating our key business metrics to improve their accuracy. Our key business metrics may differ from estimates published by third parties or from similarly titled metrics of our competitors due to differences in methodology or we may discover inaccuracies in our process for calculating such metrics. For example, during the quarter ended March 31, 2022, we experienced a system error that caused the calculation of our paying customers for such quarter to be overstated by 5, 925 pay- as- you- go customers. If investors or analysts do not perceive our key business metrics to be accurate representations of our business, or if we discover material inaccuracies in our key business metrics, our reputation, business, results of operations, and financial condition would be harmed. 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 financed our operations primarily through the sale of our equity and equity- linked securities as well as payments received from customers using our global cloud network and products. For example, we received substantial proceeds from the issuance and sale of our Class A common stock in our initial public offering ~~(IPO)~~ and in the issuances and sales of our 0. 75 % Convertible Senior Notes due 2025 (the 2025 Notes) and 0 % Convertible Senior Notes due 2026 (the 2026 Notes ~~, and together with the~~ **). We also entered into a senior secured credit agreement in May** ~~2025~~ **2024** ~~Notes,~~ **that includes a $ 400 million revolving credit facility (** the ~~Notes~~ **Revolving Credit Facility** ). Although we currently anticipate that our existing cash, cash equivalents, ~~and~~ available- for- sale securities **, available borrowing under the Revolving Credit Facility** , and cash flow from operations will be sufficient to meet our working capital and capital expenditure needs for at least the next 12 months, 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, and operating performance, and the 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. For example, volatility in equity capital markets has adversely affected and may continue to adversely affect market prices of our shares of Class A common stock. This may materially and adversely affect our ability to fund our business through the sale of our equity and equity- linked securities if such funding were to become necessary. If we raise additional funds through the issuance of equity, equity- linked or debt securities, those securities may have rights, preferences or privileges senior to the rights of our Class A common stock, and, in the case of equity or equity- linked securities, our stockholders may experience dilution. Risks Related to Our Network and Products We may not be able to respond to rapid technological changes or develop new products and product features that are attractive to, and that contain all of the capabilities required by, our current and prospective future customers, especially large customers. The industry in which we compete is characterized by rapid technological change, including frequent introductions of new products and services, evolving industry standards, changing regulations, and the development of novel cyber attacks by hostile parties, as well as changing customer needs, requirements, and preferences. Our need for continuous innovation is driven not only by competitive forces within our industry but also by our need to out- innovate the highly motivated third parties seeking to breach or compromise our network and those of our customers for economic, political, military, or other purposes. Our ability to attract new customers and retain, and increase, revenue from existing customers will depend in significant part on our ability to anticipate and respond effectively to these forces on a timely basis and continue to introduce enhancements to our network and existing products and develop new products that have the features, and that function with the security, performance, and reliability capabilities, demanded by our customers, especially our large customers. If new technologies or advancements in technologies emerge that deliver competitive products and services at lower prices, more efficiently, more conveniently, more securely or reliably, or are higher performing, these technologies or advancements could render our network and existing products less attractive to our current and prospective future customers, or obsolete. For example, artificial intelligence and machine learning may change the way our industry identifies and responds to cyber threats, and businesses that are slow to adopt or fail to adopt these new technologies may face a competitive disadvantage. The development of novel attacks or exploits by criminal or malicious elements or hostile state actors also could render our network and existing products less effective or obsolete. If we are unable to develop new products and enhance our existing products so that they have the features and capabilities required by existing and potential new customers, especially large customers, our business, results of operations, and financial condition will be materially and adversely affected. The success of our business also depends on our continued investment in our research and development organization to increase the integrity, reliability, availability, and scalability of our products. We may experience difficulties with development, design, or marketing of such enhancements to our network and products that could delay or prevent their development, introduction, or implementation. For example, in the past we have announced the development of new products and features or the release of new products or features for beta testing and the timing for the general release of the product or feature has been substantially later than we initially expected. We also have in the past experienced delays in the planned expansion of our network and in our internally planned or publicly announced

release dates of new products and new features and capabilities, and there can be no assurance that planned expansions of our network will occur on schedule and that new products, features, or capabilities will be released according to schedule or, when released, will function fully as expected. Any such delays could result in adverse publicity or brand reputation, loss of revenue or market acceptance, or claims by customers brought against us, all of which could have a material and adverse effect on our reputation, business, results of operations, and financial condition. Problems with our internal systems, networks, or data, including actual or perceived breaches or failures, could cause our network or products to be perceived as insecure, underperforming, or unreliable, our customers to lose trust in our network and products, our reputation to be damaged, and our financial results to be negatively impacted. We face security threats from malicious third parties that could obtain unauthorized access to our internal systems, networks, and data, including the equipment at our network and core co- location facilities. It is virtually impossible for us to entirely mitigate the risk of these security threats and the security, performance, and reliability of our network and products has been in the past, and may be in the future, disrupted by third parties, including nation- states, competitors, hackers, disgruntled employees, former employees, or contractors. For example, in November 2023, we detected that a likely nation- state threat actor had gained unauthorized access to one of our internal systems. While we immediately began investigating the intrusion and believe we cut off the threat actor' s access prior to significant impact on our customer data or systems, we expect we will continue to be subject to similar threats of unauthorized access in the future and we may not be as successful in quickly identifying such intrusions and mitigating the impacts of such intrusions. We also face the possibility of security threats from other sources, such as employee or contractor errors (such as errors in utilizing artificial intelligence or machine learning in our products or in the operation of our business) or malfeasance. For example, hostile third parties, including nation- states, may seek to bribe, extort, or otherwise manipulate our employees or contractors to compromise our network and products. In addition, as our business grows and we employ more employees and engage more contractors in more countries around the world, our ability to supervise the actions of our employees and contractors will decrease and the risk of an employee or contractor error or act of malfeasance will increase. These security threats from third parties are also likely to increase as the numbers, sizes, and types of customers using our network and products increases, particularly our customers that are involved in particularly sensitive industries or activities, such as banking and finance companies and governmental entities or in relation to elections in the United States or elsewhere. Additionally, artificial intelligence and machine learning may increase cybersecurity risks we face through, for example, being used to increase the prevalence or intensity of cyber attacks. While we have implemented security measures internally and have integrated security measures into our network and products, these measures have not always functioned as expected and have not always detected or prevented all unauthorized activity, prevented all security breaches or incidents, mitigated all security breaches or incidents, or protected against all attacks or incidents and these types of security failures could occur again in the future. For example, we have experienced multiple social engineering attacks where third parties have attempted, and in limited cases succeeded, in breaching our network perimeter security. While these attacks did not effectively get beyond our network perimeter security and we have not suffered any material consequences as a result of these breaches, we cannot be certain that future breaches will be avoided or, if future breaches are successful, that we will not experience material detrimental impacts, particularly if those breaches involve third party access to decrypted or other sensitive data. In addition, there is risk that the vendors we use may be attacked and the controls we have in place are bypassed and our data accessed as a result. For example, one of the IT tools our employees used internally until the first quarter of 2023 was the subject of a large security incident in December 2022, which resulted in unauthorized parties stealing large amounts of the IT tools' customers' data, including our data. We are not aware of any of our systems having been compromised as a result of this security incident due to additional required authorization and authentication events we have in place, particularly when accessing sensitive systems and resources, and we have since changed to using a new IT tool internally. In addition, in March 2022 and October 2023, breaches of the systems of our **former** identity access management vendor resulted in attacks on our systems. While we quickly discovered these resulting attacks on our systems and believed we had fully contained their impact on our systems and data, the October 2023 breach of our systems contributed to the November 2023 intrusion of our systems by a likely nation- state threat actor. While none of these incidents had a material impact on our business, results of operations or financial condition, we cannot be certain that compromises of our systems will not happen in the future as a result of these incidents or other similar incidents with third party vendors that we use to help secure our internal systems and that such incidents will not have a material impact on our results of operations or financial condition. Such incidents, whether or not successful, could result in our incurring significant costs related to, among other things, changes to our internal systems, remediating or replacing equipment within our global network, implementing additional threat protection measures, making modifications to our products and our global network, defending against litigation, responding to regulatory inquiries or actions, paying damages, providing customers with credits under our agreements with them or other incentives to maintain a business relationship with us, or taking other remedial steps with respect to third parties, as well as incurring significant reputational harm. Because these threats are constantly evolving, we believe successfully defending against them or implementing adequate preventative measures will become increasingly challenging. The global network that we use to provide our products to our customers is made up of equipment at co- location facilities located in more than ~~310~~ **335** cities and over ~~120~~ **125** countries worldwide and we expect to continue to increase the size of our network in the future. As we grow the size and scope of our network, the number of our employees and third party contractors that have access to our equipment at these facilities will continue to increase, which will also increase the risk of potential errors or malfeasance such as potential equipment theft or potential attempts to interfere with, or intercept, network and customer data that is held in, or flows through, this equipment. In addition, local government officials may attempt to, or successfully take control of, our equipment in an attempt to interfere with our services or intercept data. Because the equipment in our network co- location facilities is designed to run all of our products, any insertion of ransomware or other malicious code on, unauthorized access to, or other security breach or incident with respect to, any of this equipment at any of these locations around the world could potentially

impact all of our products running on this equipment around the world. We may also experience security breaches and other incidents that may remain undetected for an extended period and, therefore, may have a greater impact on our products and the networks and systems used in our business, the proprietary and other confidential data contained on our network or otherwise stored or processed in our operations, and ultimately our business. We expect to incur significant costs in our efforts to detect and prevent security breaches and other security- related incidents, and we have in the past faced, including in connection with the November 2023 intrusion of our systems, and may in the future face, increased costs in the event of actual or perceived security breaches or other security- related incidents. Our internal systems are exposed to the same cybersecurity risks and consequences of a breach as the systems of our customers and other enterprises, any of which could have an adverse effect on our business or reputation. These cybersecurity risks pose a particularly significant risk to a business like ours that is focused on providing highly secure products to customers. With the increase in remote work during recent years, we and our customers face increased risks to the security of infrastructure and data, and geopolitical tensions or events such as the ~~Hamas- Israel~~ **conflicts in the Middle East** and ~~Russia-~~ Ukraine ~~conflicts~~ also may increase these risks. We cannot guarantee that our security measures will prevent security breaches or incidents. We also may face increased costs relating to maintaining and securing our infrastructure and data that we maintain and otherwise process. There can be no assurance that any security measures that we or our third- party service providers have implemented or that are included in the equipment and related third- party software that we use to operate our global network will be effective against current or future security threats. We also cannot guarantee that our systems and networks or those of our third- party service providers or the equipment and related third- party software that we use to operate our global network have not been breached or otherwise compromised, or that they and any software in our or their supply chains do not contain bugs, vulnerabilities, or compromised code that could result in a breach of or disruption to our systems and networks or the systems and networks of third parties that support us and our services. Unauthorized access to, other security breaches of, or security incidents affecting, systems, networks, equipment, and data used in our business, including those of our vendors, contractors, or those with which we have strategic relationships, even if not resulting in an actual or perceived introduction of ransomware, malware, or other malicious code or other actual or perceived breach of our customers' networks, systems, or data, could result in the loss, compromise, corruption or other unavailability of data, disruptions to our and our customers' products, systems, networks, and operations, loss of business, reputational damage adversely affecting customer or investor confidence, regulatory investigations and orders, litigation, indemnity obligations, damages for contract breach, penalties for violation of applicable laws or regulations, significant costs for remediation, and other liabilities. Additionally, even in the absence of malicious actions, our network and products may experience errors, failures, vulnerabilities, or bugs that cause our products not to perform as intended and the likelihood of these problems may increase as we continue to expand the number and complexity of our products and related features, through artificial intelligence or otherwise, that we offer to our customers through our global network. For example, from time to time we are subject to " route leaks " that involve the accidental or, less commonly, illegitimate advertisement of prefixes, or blocks of IP addresses, which propagate across networks such as ours and can lead to incorrect routing of traffic across our network, taking traffic offline, or in extreme cases, potential interception of customers' traffic by attackers. For example, in June 2019, a route leak spread by a major telecommunications services provider caused significant disruption to our traffic and that of many other providers. Although events like this are outside our control, they could materially harm our reputation and diminish the confidence of our current and potential customers in our network and products. Deployment of our network and products into other computing environments may expose these errors, failures, vulnerabilities, or bugs in our products. In addition, any such errors, failures, vulnerabilities, or bugs may not be found until after they are deployed to our customers and may create the perception that our network and products are insecure, underperforming, or unreliable. For example, we have experienced a limited number of network outages over the past five years due to a variety of causes. While the June 2019 route leak and the network outages did not have a material impact on our business, results of operations or financial condition, any similar events that may occur in the future may have a material adverse impact on our results of operations or financial condition. In addition, in the event network outages or similar events occur, these events can require additional capital expenditures to lessen the chance that similar events will occur in the future. We also provide frequent updates and enhancements to our network and products, which increase the possibility of errors. Our quality assurance procedures and efforts to report, track, and monitor issues with our network has not always been sufficient to ensure we detect any such defects in a timely manner. For example, in the past we have made errors that have contributed to outages on our global network or to the leak of customer data. There can be no assurance that our software code is or will remain free from actual or perceived errors, failures, vulnerabilities, or bugs, or that we will accurately route or process all requests and traffic on our network. Given the trillions of Internet requests that route through our network on a monthly basis and the large array of Internet properties (e. g., domains, websites, APIs, and mobile applications) we service, the impact of any such error, failure, vulnerability, or bug can be large in terms of absolute numbers of affected requests and customers. Actual or perceived problems with our network or systems, or those of our vendors, contractors, or those with which we have strategic relationships, could result in actual or perceived breaches of our or our customers' networks and systems or data and / or subject us to reputational or financial harm. We are also required to comply with complex and evolving laws, regulations, and standards in many jurisdictions, including regarding our notifications to government agencies or public disclosures with respect to actual or perceived cybersecurity or personal data breaches, or other cybersecurity incidents, which could subject us to additional liability and reputational harm or lead to claims and litigation, indemnity obligations, regulatory reporting and / or audits, proceedings, and investigations and significant legal fees, significant costs for remediation, the expenditure of significant financial resources in efforts to analyze, correct, eliminate, remediate, or work around errors or defects, to address and eliminate vulnerabilities, and to address any applicable legal or contractual obligations relating to any actual or perceived security breach or incident. Our compliance efforts are complicated by the fact that these requirements and obligations may be subject to uncertain or inconsistent interpretations and enforcement, and may conflict among various jurisdictions. Actual or perceived breaches or

other security incidents could also damage our relationships with our existing customers and have a negative impact on our ability to attract and retain new customers. Because our business is focused on providing secure and high performing network services to our customers, we believe that our products and the networks and systems we use in our business could be targets for hackers and others, and that an actual or perceived breach of, or security incident affecting, our networks, systems, or data, could be especially detrimental to our reputation, customer and channel partner confidence in our solution, and our business. Additionally, our products are designed to operate without interruption, including up to a 100 % uptime guarantee for our Business and Enterprise plans. If a breach or security incident were to impact the availability of our network and products, our business, results of operations, and financial condition, as well as our reputation, could be adversely affected. Any cybersecurity insurance that we carry may be insufficient to cover all liabilities incurred by us in connection with any privacy or cybersecurity incidents or may not cover the kinds of incidents for which we submit claims. For example, insurers may consider cyber attacks by a nation- state as an " act of war " and any associated damages as uninsured. We also cannot be certain that our insurance coverage will be adequate for data handling or data security liabilities actually incurred, that insurance will continue to be available to us on economically reasonable terms, or at all, or that any insurer will not deny coverage as to any future claim. The successful assertion of one or more large claims against us that exceed available insurance coverage, or the occurrence of changes in our insurance policies, including premium increases or the imposition of large deductible or co- insurance requirements, could have a material adverse effect on our business, results of operations, and financial condition, as well as our reputation. If our global network that delivers our products or the core co- location facilities we use to operate our network are damaged, interfered with, or otherwise fail to meet the requirements of our business or local regulations, our ability to provide access to our network and products to our customers and maintain the performance of our network could be negatively impacted, which could cause our business, results of operations and financial condition to suffer. As of December 31, ~~2023~~ **2024** , we hosted our global network and served our customers from co- location and Internet Service Provider (ISP) partner facilities located in more than ~~310~~ **335** cities and over ~~120~~ **125** countries worldwide. In addition to these global facilities, much of the infrastructure for our global network and for our business and operations is maintained through a core co- location facility located in the greater Portland, Oregon area, a second core co- location facility located in ~~Luxembourg~~ **Amsterdam** that provides certain redundancy to the U. S. core facility, and through a limited number of other U. S. co- location facilities that provide limited subsets of our network support. While we have electronic and, to a lesser extent, physical access to the components and infrastructure of our network and co- location facilities that are hosted by third parties — including ISP- partner facilities — we do not control the operation of these third- party facilities. Consequently, we may be subject to service disruptions as well as failures to provide adequate support for reasons that are outside of our direct control. All of our co- location and ISP- partner facilities and network infrastructure are vulnerable to damage or interruption from a variety of sources including earthquakes; weather events; floods; fires; power loss; system failures; computer viruses; physical or electronic break- ins; human error; malfeasance; or interference, including by disgruntled employees, former employees, or contractors; **military conflicts;** terrorism; and other catastrophic events. For example, in November 2023, our control plane and analytics services experienced an outage triggered by a power failure at one of our core data centers in the greater Portland, Oregon area, which impacted certain customers' access to some of our products and services for several days and the loss of certain customer logs. In **March 2024, a subsequent power failure occurred at the same core data center in the greater Portland, Oregon area, which impacted certain customers' access to some of our products for minutes and to our analytics services for several hours. In** addition, we have experienced a route leak and a limited number of network outages involving our core and network co- location facilities over the past five years due to a variety of causes. Co- location facilities housing our network infrastructure may also be subject to local governmental or other administrative actions, changes to legal or permitting requirements, labor disputes, and litigation to stop, limit, or delay operations. Despite precautions taken at these facilities, such as disaster recovery and business continuity arrangements, the occurrence of a natural disaster or an act of **war or** terrorism, a decision to close the co- location facilities without adequate notice, interference with, or sabotage of, our equipment at these facilities, or other unanticipated problems at these facilities could result in interruptions or delays in the availability of our network and products, impede our ability to scale our operations, or have other adverse impacts upon our business, results of operations, and financial condition. In addition, errors or defects in our customers' software can result in unexpected and unintentional upward spikes in their usage of our products and network, and those spikes can cause strains on, and adversely affect the availability and functioning of, our co- location facilities and our network. As we have expanded our global network, for efficiency reasons we have increased the amount of automation that is used to update and maintain our network. While we believe this increased automation generally makes our network more reliable and robust, if portions of this automation were to fail then the impact could apply to all or substantially all of our co- location facilities, instead of the more localized impact if we were not using automation. In addition, the components of our global network are interrelated, such that disruptions or outages affecting one or more of our network co- location facilities may increase the strain on other components of our network. Concurrent disruptions or outages at one or more of our network co- location facilities may lead to a cascading effect in which heightened strain on our network causes further disruptions or outages, particularly within the regions where the disruptions and outages occur. In addition, the failure of any of our core co- location facilities for any significant period of time, particularly our U. S. core co- location facility, could place a significant strain upon the ongoing operation of our business, as we have only limited redundant functionality for these facilities. Such a failure of a core co- location facility could degrade and slow down our network, reduce the functionality of our products for our customers, result in gaps or loss in customer analytics or functionality with respect to some of our products, impact our ability to bill our customers, result in the loss of customers or reduction in their purchases from us due to dissatisfaction with the reliability of our products and network, and otherwise materially and adversely impact our business, reputation, and results of operations. If our customers' or partners' access to our network and products is interrupted or delayed for any reason, our business could suffer. Any interruption or delay in our

customers' or partners' access to our network and products will negatively impact our customers. Our customers depend on the continuous availability of our network for the delivery and use of our products, and our products are designed to operate without interruption, including up to 100 % uptime guarantee for our Business and Enterprise plans. If all or a portion of our network were to fail, our customers and partners could lose access to their internal network and / or the Internet as a whole until such disruption is resolved or they deploy disaster recovery options that allow them to bypass our network. The adverse effects of any network interruptions on our reputation and financial condition may be heightened due to the nature of our business and our customers' expectation of continuous and uninterrupted Internet access and low tolerance for interruptions of any duration. In addition, because some of our customers' most critical applications are protected by our products and network and these customers may not be using other providers for similar services, the adverse effect of network disruptions to these customers could be particularly severe. The impact of an interruption in access to our network and products could also impact the ability to run our own business because we use a number of our products in the operation of our business. While we do not consider them to have been material, we have experienced a limited number of network outages over the past five years, and we may in the future experience network disruptions and other performance problems, in each case due to a variety of factors. The following factors, many of which are beyond our control, can affect the delivery, performance, and availability of our network and products: • the development, maintenance, and functioning of the infrastructure of the Internet as a whole; • the performance and availability of third- party telecommunications services with the necessary speed, data capacity, and security for providing reliable Internet access and services; • decisions by the owners and operators of the co- location and ISP- partner facilities where our network infrastructure is deployed or by global telecommunications service provider partners who provide us with network bandwidth to terminate our contracts, discontinue services to us, shut down operations or facilities, increase prices, change service levels, limit bandwidth, declare bankruptcy, breach their contracts with us, or prioritize the traffic of other parties; • the occurrence of earthquakes, floods, weather events, fires, power loss, system failures, physical or electronic break- ins, acts of war or terrorism (including the ongoing conflicts **in the Middle East** ~~between Hamas and Israel and between Russia~~ and Ukraine or potential consequence of geopolitical tensions in other areas of the world), human error or interference (including by disgruntled employees, former employees, or contractors), and other catastrophic events; • cyber attacks targeted at us, facilities where our network infrastructure is located, our global telecommunications service provider partners, or the infrastructure of the Internet; • errors, defects, or performance problems in the deployment, maintenance, and expansion of our network and products, including the software we **develop or license from third parties and** use to operate our network and products and provide ~~our~~ **such** related products to our customers; • our customers' or partners' improper deployment or configuration of our customers' access to our network and products; • the maintenance of the APIs in our systems that our partners use to interact with us; • the failure of our redundancy systems, in the event of a service disruption at one of the facilities hosting our network infrastructure, to redistribute load to other components of our network; and • the failure of our disaster recovery and business continuity arrangements. The occurrence of any of these factors, or our inability to efficiently and cost- effectively fix such errors or other problems that may be identified, could damage our reputation, negatively impact our relationship with our customers, or otherwise materially harm our business, results of operations, and financial condition. Abuse, misuse, or other unauthorized use of our internal network, including network services tools, could cause significant harm to our business and reputation. Our employees and contractors use our internal network to support the operation of our global network and products for our customers. In addition, in order to provide real- time support to our customers, we have created internal network services tools that are used by our employees and contractors to diagnose and correct customer security, performance, and reliability issues. If any of our employees or contractors were to intentionally abuse our internal network, including these tools, by interfering with or altering our customers' Internet properties or systems, our customers could be significantly harmed. Similarly, our customers could be harmed if government personnel in any countries in which our employees operate were to pressure our employees, including through the threat of potential prosecution or imprisonment, to use our internal network, including these tools, to access customer data or interfere with or alter our customers' Internet properties or systems. Our employees' inadvertent misuse of our internal network, including these tools, could similarly harm our customers. For example, third parties have in the past attempted to induce our employees to use their administrative access to reveal, remove, or disable our customers' information and content, including by submitting fraudulent law enforcement requests, copyright takedown requests, or other content- based complaints. Any such improper disclosure or removal could significantly and adversely impact our business and reputation. While our internal network and tools have been developed only for authorized use by our employees and contractors, any unauthorized use of, or access to, our internal network by, or release of network service tools to, third parties would represent a significant vulnerability in our products. Accordingly, any abuse or misuse of our internal network and services tools could significantly harm our business and reputation. If it became necessary to further restrict the availability or use of our internal network and services tools by our employees and customers in response to any abuse or misuse, our ability to deliver high- quality and timely customer support could be harmed. Detrimental changes in, or the termination of, any of our co-location relationships, ISP partnerships, or our other interconnection relationships with ISPs could adversely impact our business, results of operations, and financial condition. Our relationships with ISP partners and other vendors that provide co-location services for our network infrastructure and the pricing and other material contract terms we have with these vendors are important for the maintenance, development, and expansion of our global network. If any of our co- location agreements were to expire or the pricing and other material terms of these agreements were to worsen, our business, results of operations, and financial condition would be adversely affected unless we were able to find a substitute vendor for the impacted facility on comparable or better terms. Moreover, a significant number of our important co- location agreements are with a single company and if our arrangements with this company were to change in a manner adverse to us, we could face difficulty in maintaining or growing our network on commercially viable terms. In addition, as part of our arrangements with some of our ISP partners, the ISP partner has agreed to host our equipment for free or at a discount to the partner' s customary rate. There can be no

assurances that these ISP partners will continue to provide these types of favorable equipment hosting arrangements in the future. The efficient and effective operation of our network also relies upon a series of mutually beneficial arrangements with other Internet infrastructure companies. These arrangements are often referred to as " peering " or " interconnection " agreements ~~,~~ and allow us and our ISP partners to reduce bandwidth costs related to operating our respective networks. If the underlying competitive, business, or operational incentives supporting these arrangements were to change, we or our partners might terminate these agreements or allow them to expire. Many of our peering or interconnection agreements have a term of three years or less, after which such agreements auto- renew on an annual basis. Changes to the underlying incentive structure of peering arrangements may result from parties seeking to take advantage of an essential position or enter into exclusive arrangements, changes to U. S. or international laws, regulations, or policies, increasing competition between us and these Internet infrastructure providers, or changes in the norms governing the relationships among Internet infrastructure providers. Without favorable peering arrangements, we would incur significantly increased costs to continue to provide our products at their current levels and such increased costs could adversely impact our business, results of operations, and financial condition. In addition, to the extent that additional countries begin to regulate peering with outside networks, our costs may increase and our business and results of operations could be adversely impacted. If our network and products do not interoperate with our customers' internal networks and infrastructure or with third- party products, websites, or services, our network may become less competitive and our results of operations may be harmed. Our network and products must interoperate with our customers' existing internal networks and infrastructure. These complex internal systems are developed, delivered, and maintained by the customer and a myriad of vendors and service providers. As a result, the components of our customers' infrastructure have different specifications, rapidly evolve, utilize multiple protocol standards, include multiple versions and generations of products, and may be highly customized. We must be able to interoperate and provide products to customers with highly complex and customized internal networks, which requires careful planning and execution between our customers, our customer support teams and, in some cases, our channel partners. Further, when new or updated elements of our customers' infrastructure or new technology or industry standards or protocols are introduced, we may have to update or enhance our network to allow us to continue to provide our products to customers. Our competitors or other vendors may refuse to work with us to allow their products to interoperate with our network and products, which could make it difficult for our network and products to function properly in customer internal networks and infrastructures that include these third- party products. We may not deliver or maintain interoperability quickly or cost- effectively, or at all. These efforts require capital investment and engineering resources. If we fail to maintain compatibility of our network and products with our customers' internal networks and infrastructures, our customers may not be able to fully utilize our network and products, and we may, among other consequences, lose or fail to increase our market share and number of customers and experience reduced demand for our products, which would materially harm our business, results of operations, and financial condition. Because we provide some of our products through a reverse- proxy, which is a network arrangement in which Internet user requests initially are directed to our network' s servers rather than those of our customers, the source of some traffic may be difficult to ascertain. When they cannot identify the source of the traffic, some governments, third- party products, websites, or services may block our traffic or blacklist our IP addresses. If our customers experience significant instances of traffic blockages, they will experience reduced functionality or other inefficiencies, which would reduce customer satisfaction with our network and products and likelihood of renewal of their use of our products. We rely on a limited number of suppliers for certain components of the equipment we use to operate our network and any disruption in the availability **, or price,** of these components could delay our ability to expand or increase the capacity of our global network ~~or~~ **,** replace defective equipment **, or identify alternative supply sources favorable to us** . We rely on a limited number of suppliers for several components of the equipment we use to operate our network and provide products to our customers. Our reliance on these suppliers exposes us to risks, including reduced control over production costs **, increased prices due to tariffs,** and constraints based on the then **-** current availability, terms, and pricing of these components. For example, we generally rely on a limited number of suppliers for the servers that we use in our network and we ordinarily purchase these components on a purchase- order basis, without any long- term contracts guaranteeing supply. **We may also be subject to price increases from these suppliers should they be negatively impacted by tariffs or other regulations.** While the network equipment and servers we purchase generally are commodity equipment and we believe an alternative supply source **or location** for servers on substantially similar terms could be identified quickly, our business could be adversely affected until those efforts are completed. In addition, the technology equipment industry has experienced component shortages and delivery delays in the past, and we may experience shortages or delays, including as a result of natural disasters, increased demand in the industry, **military conflicts and geopolitical tensions, labor strikes, or other related conditions,** or our suppliers lacking sufficient rights to supply the components in all jurisdictions in which we have co- location facilities that support our global network. For example, during 2021 and continuing through the first quarter of 2022, a global shortage of CPUs, RAM, SSDs, and other electronics resulted in supply constraints for a number of electronics firms, including manufacturers of servers. This global shortage disrupted **and increased the cost** , and other shortages or similar supply constraints in the future may disrupt **or increase the cost** , **of** some of our expected purchases of network equipment and servers. If our supply of certain components is disrupted or delayed **or becomes more expensive** , there can be no assurance that additional supplies or components can serve as adequate replacements for the existing components or that supplies will be available on terms that are favorable to us, if at all. Any disruption or delay **or additional costs** in the supply of our hardware components may delay the opening of new co- location facilities, limit capacity expansion or replacement of defective or obsolete equipment at existing co- location facilities, ~~or~~ cause other constraints on our operations that could damage our customer relationships **, or otherwise adversely impact our business, financial condition, or results of operations** . The actual or perceived failure of our products to block malware or prevent a security breach or incident could harm our reputation and adversely impact our business, results of operations, and financial condition. Our security products are designed to reduce

the threat to our customers posed by malware and other Internet security threats. Our security products may fail to detect or prevent malware or security breaches or incidents for any number of reasons. Even where our security products perform as intended, the performance of our security products can be negatively impacted by our failure to enhance, expand, or update our network and products; improper classification of websites by our employees, automated systems, and partners which identify and track malicious websites; improper deployment or configuration of our products; the development, maintenance, and functioning of the infrastructure of the Internet as a whole; and many other factors. For example, during August and September of 2023, an unknown threat actor exploited a vulnerability in the standard HTTP / 2 protocol critical to the function of the Internet and websites. This threat actor worked to generate a series of the largest- scale DDoS attacks against our network that we have recorded **prior** to ~~date~~ **that time** . While our systems were able to mitigate the overwhelming majority of incoming attacks, the volume overloaded some components in our network and impacted several customers' performance, all of which were quickly resolved. During the process of mitigating these attacks, our team developed new technology to stop these types of attacks and further improve our own mitigations for this and other future attacks. Although the impact of the attacks did not have a material impact on our reputation or results of operations or financial condition, other future attacks like these may materially and adversely impact our reputation, results of operations or financial condition if we cannot effectively stop or mitigate the attacks and otherwise suffer performance issues or downtime that exceeds the service level commitments under our agreements and terms of service with our paying customers. Companies are increasingly subject to a wide variety of attacks on their networks and systems, including traditional computer hackers; malicious code, such as viruses and worms; DDoS attacks; sophisticated attacks conducted or sponsored by nation- states; advanced persistent threat intrusions; ransomware; phishing attacks and other forms of social engineering; employee, vendor, or contractor errors or malfeasance; and theft or misuse of intellectual property or business or personal data, including by disgruntled employees, former employees, or contractors. External events, like the ongoing conflicts **in the Middle East** ~~between Hamas and Israel and between Russia~~ and Ukraine and other areas of geopolitical tension around the world and elections in the United States and elsewhere, can increase the likelihood of attacks. No security solution, including our products, can address all possible security threats or block all methods of penetrating a network or otherwise perpetrating a security incident. Accordingly, our security products may be unable to detect or prevent a threat until after our customers are impacted. As our products are adopted by an increasing number of enterprises and by increasingly larger enterprises, it is possible that the individuals and organizations behind cyber threats will focus on identifying ways to circumvent or defeat our security products. If our network is targeted by attacks specifically designed to disrupt it, it could create the perception that our security products are not capable of providing adequate security. As a provider of security products, any perceived lack of security to our network or any of our products could erode our customers' and potential customers' trust in our network and products. Moreover, a high- profile security breach of, or security incident impacting, another cloud services provider could cause our customers and potential customers to lose trust in cloud solutions generally, and cloud- based products like ours in particular. Any such loss of trust could materially and adversely impact our ability to retain existing customers or attract new customers. Our customers must rely on complex network and security infrastructures, which include products and services from multiple vendors in addition to us, to secure their networks. If any of our customers becomes infected with malware, or experiences a security breach or incident, they could be disappointed with our products, regardless of whether our security products are intended to block the attack or would have blocked the attack if the customer had properly configured our products or their network, or taken other steps within their control. Additionally, if any enterprises that are publicly known to use our network and products are the subject of a cyber attack that becomes publicized, this could harm our reputation and our current or potential customers may look to our competitors for alternatives to our network and products. Customers subject to cyber attack also may seek to hold us legally liable for any loss or lack of access to sensitive data or highly valued assets that results from such an attack. Although our customer agreements provide significant limitations on our potential liability to our customers for such claims and we do not believe current legal theories would hold a service provider like us liable for such customers' losses, potential adverse future changes in laws applicable to such claims could result in significant liabilities for us. From time to time, industry or financial analysts and research firms test our network and related security products against other security products. Our products may fail to detect or prevent threats in any particular test for a number of reasons, including misconfiguration. To the extent potential customers, industry or financial analysts, or testing firms believe that the occurrence of a failure to detect or prevent any particular threat is a flaw or indicates that our products do not provide significant value or provide less value than competitive solutions, our reputation and business could be materially harmed. Any real or perceived flaws in our network, or any actual or perceived security breaches of, or security incidents impacting, our customers, could result in: • a loss of existing or potential customers or channel partners; • delayed or lost sales and harm to our financial condition and results of operations; • a delay in attaining, or the failure to attain, market acceptance of our products; • the expenditure of significant financial resources in efforts to analyze, correct, eliminate, remediate, or work around errors or defects, to address and eliminate vulnerabilities, and to address any applicable legal or contractual obligations relating to any actual or perceived security breach or incident; • negative publicity and damage to our reputation and brand; and • legal claims and demands (including for stolen assets or information, repair of system damages, and compensation to customers and business partners), litigation, regulatory audits, proceedings or investigations, and other liability. Any of the above results could materially and adversely affect our business, results of operations, and financial condition. We may choose to make public disclosures in press releases, on our website and blog, through social media, and in other ways about our network, systems, products, and technology, which may include negative events, when we are not otherwise required by applicable law and those disclosures could materially and adversely impact our business, reputation, and results of operations. In the past we have been, and in the future we expect to be, transparent about our network, systems, products, and technology with our customers and the public in general. We believe that being rigorously and promptly transparent is an essential part of maintaining trust with our customers. At times, this transparency may result in us publicly disclosing information, including

negative events, about our network, systems, products, and technology in circumstances where we may not be required to do so by applicable law. If and when we choose to make these types of non- legally required public disclosures, we may suffer reputational damage, loss of existing and potential new customers, litigation, indemnity obligations, damages for contract breach, penalties for violation of applicable laws or regulations, significant costs for remediation, and other liabilities that could materially and adversely impact our business, reputation, and results of operations. In addition, we face increasing regulation requiring notifications to government agencies and / or public disclosures with respect to cybersecurity, critical infrastructure, privacy and data protection, and other incidents. If we do not believe the requirements of an applicable regulation have been triggered by an incident but we otherwise make a public disclosure about the incident, then one or more government regulators may seek additional information about the incidents or may allege that we failed to comply with our notification obligations to such agency or under applicable law. Such allegations could result in harm to our reputation, distraction to our senior management team, potential investigations and fines, and loss of customers, or result in other liabilities or adverse consequences on our business. We provide service level commitments under our Enterprise subscription plan customer contracts and our Business subscription plan terms of service. If we fail to meet these contractual commitments, we could be obligated to provide credits for future service or allow customers to terminate their subscriptions and our business could suffer. Our Enterprise subscription plan agreements and our Business subscription plan terms of service typically provide for service level commitments, which contain specifications regarding the availability and performance of our network. In particular, our Enterprise subscription plan and our Business subscription plan terms of service include up to a 100 % uptime guarantee. Any failure of or disruption to our infrastructure could adversely impact the security, performance, and reliability of our network and products for our customers. If we are unable to meet our stated service level commitments or if we suffer extended periods of poor performance or unavailability of our network and products, these customers could seek to bring claims against us or terminate their agreements with us and, in the case of our contracted customers, we may be contractually obligated to provide affected customers with service credits that they may apply against future subscription fees otherwise owed to us, and, in certain cases, refunds of pre- paid and other fees. For example, a route leak and a limited number of network outages during the past five years triggered certain of these types of obligations. Although the impact of the route leak and these outages did not have a material impact on our results of operations or financial condition, other future events like these may materially and adversely impact our results of operations or financial condition. Our revenue, other results of operations, and financial condition could be harmed if we suffer performance issues or downtime that exceeds the service level commitments under our agreements and terms of service with our paying customers. If our products do not obtain and maintain market acceptance, our ability to grow our business and our results of operations may be adversely affected. Our products are still evolving and it is difficult to predict customer demand and adoption rates for our product offerings. We believe that our network and cloud- based products represent a major shift from traditional solutions. Many of our potential customers, particularly large enterprises and government entities, face barriers to adopting our offerings because of their prior investment in, and the familiarity of their IT personnel with, on-premises, appliance- based solutions or other providers of cloud- based solutions. As a result, our sales process often involves extensive efforts to educate our customers about our products, particularly as we continue to pursue customer relationships with large organizations. Our customers also expect us to meet voluntary validations or adhere to industry standards and require our policies and practices to be evaluated by an independent third- party assessor. Although we currently have certain certifications and reports such as SOC2 Type 2, PCI DSS, ISO 27001, ISO 27701, and ISO 27018, C5, EU Code of Conduct, **UK Cyber Essentials, ENS** and FedRAMP moderate authorization, we may not be successful in continuing to maintain those certifications or in obtaining other certifications. In addition, sales to government entities and other large enterprises may in particular be conditioned upon adherence to PSPC, ISMAP, IRAP, or DoD IL4 compliance in Canada, Japan, Australia, and the United States, and we do not currently have these certifications. The costs of obtaining and maintaining certification pursuant to any of these standards are significant, and any failure to obtain and maintain such certifications for our network and products could reduce demand for them, which would harm our business, results of operations, and financial condition. To the extent our competitors have, and we do not have, these certifications, we may lose the opportunity to obtain subscriptions from certain potential paying customers. Despite our efforts, we can provide no assurance that our cloud- based products will obtain market acceptance or that competing products or services based on other cloud- based and / or on- premises technologies will not achieve market acceptance. If we fail to achieve market acceptance of our products or are unable to keep pace with industry changes or obtain necessary product certifications, our ability to grow our business, results of operations, and financial condition will be materially and adversely affected. In connection with our Web3 suite of products and our potential future participation in various Web3 protocol governance activities, we expect to hold certain types of cryptocurrency and similar types of digital assets that may be subject to unique regulatory ~~and accounting~~ risks, volatile market prices, and risks of loss, which could harm our business and reputation. The regulatory status of digital assets is subject to significant change. Some or all of these assets are subject to significant regulatory restrictions and have even been prohibited or effectively prohibited in some countries. If we fail to comply with regulations or prohibitions applicable to us based on these types of digital assets, we could face regulatory or other enforcement actions and potential fines and other consequences. The prices of digital assets have been and may continue to be highly volatile, including as a result of various associated risks, uncertainties and events. The prevalence of such assets is a relatively recent trend, and their long- term adoption by investors, consumers, and businesses remains uncertain ~~. For example, the bankruptcy of FTX Trading Ltd. in November 2022 undermined investor confidence in cryptocurrencies resulting in a decline in the price of cryptocurrency and similar types of digital assets~~. Moreover, digital assets' lack of a physical form, their reliance on technology for their creation, existence, and transactional validation, and their decentralization may subject their integrity to the threat of malicious attacks and technological obsolescence. In addition, if the market value of the digital assets we hold increases significantly relative to the purchase prices, we could be deemed an" investment company" for purposes of the Investment Company Act of 1940, as amended, and may be required to institute burdensome compliance requirements,

restricting our activities in a way that could adversely affect our business, financial condition, and results of operations ~~. Moreover, digital assets are currently considered indefinite- lived intangible assets under applicable accounting rules, meaning that any decrease in their fair values below our carrying values for such assets at any time subsequent to their acquisition will require us to recognize impairment charges, whereas we may make no upward revisions for any market price increases until a sale, which may adversely affect our operating results in any period in which such impairment occurs. There is no guarantee that future changes in U. S. GAAP will not require us to change the way we account for digital assets held by us~~ . Further, digital assets have been, and may in the future be, subject to security breaches, cyber attacks, or other malicious activities, including unauthorized access and theft, as well as human errors or computer malfunctions that may result in the loss or destruction of private keys needed to access such assets. While we expect to implement appropriate security measures with respect to any future digital assets holdings, those measures may not function as expected and may not detect or prevent all unauthorized activity, prevent all security breaches or incidents, mitigate all security breaches or incidents, or protect against all attacks or incidents. If such threats are realized or the measures or controls that we create or implement to secure such assets fail, it could result in a partial or total misappropriation or loss of such digital assets. Risks Related to Legal, Tax, and Regulatory Matters Activities of our paying and free customers or the content of their websites and other Internet properties may violate applicable laws and / or our terms of service and could subject us to lawsuits, regulatory enforcement actions, and / or liability in various jurisdictions. Through our network, we provide a wide variety of products that enable our customers and our customers' users to exchange information, conduct business, and engage in various online activities both domestically and internationally. Our customers and our customers' users may use our network and products in violation of applicable law or in violation of our terms of service or the customer' s own policies. The existing laws relating to the liability of providers of online products and services for activities of their users are highly unsettled and in flux both within the United States and internationally. We are currently, and in the future may be, subject to lawsuits and / or liability arising from the conduct of our customers and our customers' users. Additionally, the conduct of our customers and our customers' users may subject us to regulatory enforcement actions and / or liability. We are a defendant in lawsuits, both in the United States and abroad, seeking injunctive relief and / or damages against us based on content that is made available through our customers' websites and other Internet properties. A number of these lawsuits involve copyright infringement claims, and courts in **some countries** ~~Italy and Germany~~ have ~~at times~~ **found that we may be held liable in certain circumstances for damages arising from infringement on a customer' s website or** directed us to take action by removing access to content of certain websites and other Internet properties on our network. There can be no assurance that we will not face similar litigation in the future or that we will prevail in any litigation we are facing or may face. An adverse decision in one or more of these lawsuits could materially and adversely affect our business, results of operations, and financial condition. Several U. S. federal statutes may apply to us with respect to various activities of our customers, including the Digital Millennium Copyright Act (DMCA), which provides recourse for owners of copyrighted material who believe their rights under U. S. copyright law have been infringed on the Internet; and section 230, enacted in the Communications Decency Act (CDA), which addresses blocking and screening of content on the Internet. Although these and other similar legal provisions provide limited protections from liability for service providers like us, those protections may not be interpreted in a way that applies to us, may be amended or removed in the future, or may not provide us with complete protection from liability claims. If we are found not to be protected by the safe harbor provisions of the DMCA, CDA or other similar laws, or if we are deemed subject to laws in other countries that may not have the same protections or that may impose more onerous obligations on us, we may owe substantial damages and our brand, reputation, and financial results may be harmed. Policies and laws in this area remain highly dynamic, and we may face additional theories of intermediary liability in various jurisdictions. Many policymakers in the United States have called for a re- examination of CDA section 230 and copyright law. The ~~EU has agreed on the~~ Digital Services Act and Digital Markets Act ~~to update~~ **have gone into effect in the European Union (EU), updating** the rules governing digital services like ours ~~, including replacing the eCommerce Directive, which is the EU' s current framework for online services,~~ and imposing additional legal requirements on certain service providers. In addition, in 2019, the EU approved a Copyright Directive that will impose additional obligations on service providers and failure to comply could give rise to significant liability. Other laws and pending legislation at the EU level (terrorist content, child sexual abuse materials) and in the United Kingdom (online harms), Australia (online harms), and India (Digital India Act), as well as other new laws like them, may also expose Internet companies like us to significant liability. We may incur additional costs to comply with these new laws, which may have an adverse effect on our business, results of operations, and financial condition. Current and future litigation subjects us to claims for very large potential damages based on a significant number of online occurrences under statutory or other damage theories. Such claims may result in liability that exceeds our ability to pay or our insurance coverage. Even if claims against us are ultimately unsuccessful, defending against such claims will increase our legal expenses and divert management' s attention from the operation of our business, which could materially and adversely impact our business and results of operations. Our policies regarding user privacy could cause us to experience adverse business and reputational consequences with customers, employees, suppliers, government entities, and other third parties. As a company, we strive to protect our customers' privacy consistent with applicable law. Consequently, we generally do not provide personal information about our customers or their users without legal process. In accordance with our contractual commitments to our customers, we may need to challenge legal process requesting disclosure of personal information where such requests are inconsistent with applicable data protection laws. In addition, from time to time, government entities may seek or demand our assistance with obtaining information about our customers or their users or could request that we modify our network and products in a manner to permit access or monitoring. In light of our privacy commitments, we may legally challenge certain law enforcement requests, such as requests to provide a feed of content transiting our network, to obtain encryption keys, or to modify or weaken encryption. We also may face complaints from individuals who assert we have provided their information improperly to law enforcement or in response to third- party abuse

complaints, despite policies we have in place to protect that information. To the extent that we do not provide assistance to **,** or comply with requests from **,** government entities or challenge those requests publicly or in court, we may experience adverse political, business, and reputational consequences. We may also face such adverse political, business, and reputational consequences to the extent that we provide, or are perceived as providing, assistance to government entities that exceeds our legal obligations. For example, we periodically receive requests for information purportedly originating from law enforcement agencies or pursuant to legal process, but which are fraudulent or improper attempts to cause us to reveal customer information. Any such disclosure could significantly and adversely impact our business and reputation. We publish a transparency report on a semi- annual basis to provide details of law enforcement and government requests we receive. Our transparency report also includes a list of certain actions we have not taken in response to law enforcement requests. If we are ever required by law enforcement to take one or more of the actions covered by those disclosures, then we would have to remove the applicable disclosures from our transparency report. Both the publishing of our transparency report and, conversely, the potential narrowing of the list of actions we have not taken in response to law enforcement requests could damage our business and reputation. Our business could be adversely impacted by changes in Internet access for our customers as a result of competitive behavior or laws specifically governing the Internet. Our network performance and reliability depends on the quality of our customers' access to the Internet. Certain features of our network require significant bandwidth and fidelity to work effectively. Internet access is frequently provided by companies that have significant market power that could take actions that degrade, disrupt, or increase the cost of user access to our network, which would negatively impact our business. We could incur greater operating expenses and our customer acquisition and retention could be negatively impacted if other network operators: • implement usage- based pricing; • discount pricing for competitive products; • otherwise materially change their pricing rates or schemes; • charge us to deliver our traffic at certain levels or at all; • throttle traffic based on its source or type; • implement bandwidth caps or other usage restrictions; or • otherwise try to monetize or control access to their networks. In addition, there are various laws and regulations that could impede the growth of the Internet or online services, and new laws and regulations may be adopted in the future. These laws and regulations could involve interconnection and network management; taxation; tariffs; privacy; data protection; information security; content; copyrights; distribution; electronic contracts and other communications; consumer protection; **requirements to block certain data from being transferred to named countries or entities,** and requirements for the characteristics and quality of services, any of which could decrease the demand for, or the usage of, our products. Legislators and regulators may make legal and regulatory changes, or interpret and apply existing laws, in ways that require us to incur substantial costs, expose us to unanticipated civil or criminal liability, or cause us to change our business practices. If these changes are implemented, it could have an adverse and negative impact on our business. In addition, we may be banned from providing our products in certain countries, which would prevent our ability to grow our business in such markets and would also have a detrimental impact on the performance and scope of our network. Russia, for example, has blocked designated virtual private networks since December 2021, and included one of our products, Cloudflare WARP, in its list of banned services. These changes or increased costs could materially harm our business, results of operations, and financial condition. Failure to comply with laws and regulations applicable to our business could subject us to fines and penalties and could also cause us to lose customers or otherwise harm our business. Our business is subject to regulation by various federal, state, local, and non- U. S. governmental agencies, including agencies responsible for monitoring and enforcing compliance with various legal obligations, such as privacy, data protection, and information security laws and regulations, intellectual property laws, telecommunications laws and regulations, employment and labor laws, workplace safety, environmental laws, consumer protection laws, anti- bribery laws, governmental trade sanctions laws, import and export controls, anti- corruption and anti-bribery laws, federal securities laws, and tax laws and regulations. In addition, emerging tools and technologies we may utilize in providing our products and solutions, like artificial intelligence and machine learning, may also become subject to regulation under new laws or new applications of existing laws. In certain jurisdictions, some or all of these regulatory requirements may be more stringent than in the United States. In addition, ~~many~~ **the United States and other** countries are considering expanding or have expanded regulatory requirements for services such as ours, with potential requirements such as collection and verification of customer data, limitations on the use of non- personal data **, limitations on the transfer of certain types of data to named countries or entities** , cybersecurity incident reporting obligations, expanded registration requirements, or requirements to have personnel in the country. The rapid expansion of proposed regulations, as well as possible conflicting requirements, may make it challenging for us to identify and comply with all new global regulations that may apply to our services. These laws and regulations impose added costs on our business. Actual or perceived noncompliance with applicable regulations or requirements could subject us to: • investigations, enforcement actions, and sanctions; • mandatory changes to our network and products; • disgorgement of profits, fines, and damages; • civil and criminal penalties or injunctions; • claims for damages by our customers or channel partners; • termination of contracts; • loss of intellectual property rights; and • temporary or permanent debarment from sales to government organizations. If any governmental sanctions are imposed, or if we do not prevail in any possible civil or criminal litigation, our business, results of operations, and financial condition could be adversely affected. In addition, responding to any action will likely result in a significant diversion of our management' s attention and resources and an increase in professional fees. Enforcement actions and sanctions could materially harm our business, results of operations, and financial condition. Additionally, companies in the technology industry have recently experienced increased regulatory scrutiny. The rapid growth of our business and the products that we offer may also result in increased regulatory scrutiny of our company in particular. Any reviews by regulatory agencies or legislatures may result in substantial regulatory fines, changes to our business practices, and other penalties, which could negatively affect our business and results of operations. Changes in social, political, and regulatory conditions or in laws and policies governing a wide range of topics may cause us to change our business practices. Further, our expansion into a variety of new fields also could raise a number of new regulatory issues. These factors could negatively affect our business and results of operations in material ways. Our actual or

perceived failure to comply with privacy, data protection, information security, and other applicable laws, regulations, and obligations could harm our business. We receive, store, use, and otherwise process personal information and other information relating to individuals. There are numerous federal, state, local, and international laws and regulations regarding privacy, data protection, information security, and the storing, sharing, use, processing, transfer, disclosure, and protection of personal information and other content, the scope of which are changing, subject to differing interpretations, and may be inconsistent among jurisdictions, or conflict with other rules. Not only is the number of data protection laws rising globally and within the United States, but existing laws and regulations are evolving. Together, this legislative framework may result in ever- increasing regulatory and public scrutiny and escalating levels of enforcement and sanctions. For example, the EU' s General Data Protection Regulation (GDPR) imposes stringent data protection requirements and provides for penalties for noncompliance of up to the greater of € 20 million or four percent of worldwide annual revenues. In addition, the GDPR and the data protection laws of **numerous** ~~a number of~~ other jurisdictions such as Japan, China, ~~and~~ South Korea, **and the United Kingdom** prohibit cross- border data transfers unless certain contractual and other conditions are met. This requires us to incur substantial costs and engage in additional contract negotiations with some of our customers and vendors to ensure the conditions established by these data protection regulations are met. Some countries are also considering or have enacted legislation and / or certification schemes requiring local storage and processing of data, or other sovereignty- oriented requirements, that could increase the cost and complexity of delivering our services ~~. For example, the European Union Agency for Cybersecurity' s draft version of the European Cybersecurity Certification Scheme for Cloud Services would require EU data sovereignty for companies seeking to obtain the highest certification level~~ . In addition, the interpretation of existing privacy, data protection, and information security laws and regulations by governmental entities and the courts may change significantly over time in a manner that can have a significantly adverse impact on both our business and our customers' businesses. **This is especially true regarding the cross- border transfer of data.** For example, in ~~July 2020, the Court of Justice of the European Union (CJEU) in the" Schrems II" case invalidated the U. S.- EU Privacy Shield that was widely used by us and other companies to allow for the lawful transfer of personal data of European Economic Area (EEA) residents to the United States for processing under the GDPR and placed additional requirements on the use of the EU Standard Contractual Clauses (EU SCCs) as a mechanism for transferring EEA personal data to the United States. We incurred substantial costs and needed to engage in additional contract negotiations with some of our customers and vendors in connection with updated EU SCCs and the United Kingdom addendum to the EU SCCs or other appropriate contractual provisions that we sought to put in place with our customers and vendors. In~~ July 2023, the European Commission adopted an adequacy decision for the new EU- U. S. Data Privacy Framework, which **generally allows** ~~is designed to address~~ the ~~concerns raised in~~ **free flow of EU personal data to** the ~~Schrems II case~~ **United States for participating entities** . **While** ~~However, the European Commission' s adequacy decision regarding~~ this framework **currently** ~~will be subject to future reviews and may be subject to suspension, amendment, repeal, or limitations to its scope by the European Commission. While this new framework may serve~~ **serves** as a means for cloud service providers like our company to freely transfer EU personal data to the United States, **it** ~~many~~ **may be** ~~aspects of this new framework remain uncertain. It has already been~~ subject to **future** legal ~~challenge~~ **challenges , suspension, amendment, repeal, or limitations to its scope by the European Commission** , and some customers and vendors ~~are~~ **may be** unwilling to rely on **this** ~~the new~~ framework due to ~~this~~ **these and other** ~~uncertainty~~ **uncertainties** . In addition, in January 2023, the European Data Protection Board issued its 2022 Coordinated Enforcement Action on the use of cloud- based services by the public sector, in which it expressed concerns that EU public sector entities may not be able to use U. S.- based cloud service providers consistently with GDPR due to their concerns about the ability of U. S. government agencies to access EU personal data. ~~,laws,regulations,and industry standards concerning privacy,data protection,and information security proposed and enacted in~~ the United States and various individual U.S.states.In the United States,various federal laws and regulations already apply to the collection,processing,disclosure and security of certain types of data,including the Electronic Communications Privacy Act,the Computer Fraud and Abuse Act,the Health Insurance Portability and Accountability Act of 1996,and the Gramm- Leach- Bliley Act.In addition,there are also a number of recently enacted or proposed U.S.federal and state privacy and data protection bills in Congress and state legislatures across the country. **We are also subject to the terms of our privacy policies and contractual** ~~Obligations~~ **obligations** ~~relating~~ **to third parties related** to privacy,data protection,and information security ~~also are increasing~~ **.We strive to comply with applicable laws,regulations,policies,and other legal obligations relating to privacy,data protection,and information security to the extent possible.However,the regulatory framework for privacy and data protection worldwide is evolving rapidly,and it is possible that these or other actual or alleged obligations may be interpreted and applied** in **a manner that** ~~complexity outside the U.S.For example,the EU has revised its~~ **is** ~~Cybersecurity Directive (NIS2),which,among~~ **inconsistent from one jurisdiction to another and may conflict with** other **rules** ~~things,obligates companies to adopt or update policies and procedures on issues such as incident handling and supply chain security,implementing certain administrative measures,and requires top management' s involvement in cybersecurity risk- management measures,with top management potentially held liable for~~ **or** ~~non-~~ **our practices.As data protection** compliance ~~.NIS2 provides for~~ Whether as a result of ~~this~~ **these developments** or otherwise, we may continue to see more findings from ~~privacy~~ regulators around the world against cloud service providers relating to cross- border personal data transfers, and may find it necessary or appropriate to modify our policies and practices to address any such findings or other legislative developments relating to cross- border personal data transfers. Implementing any new guidance from applicable regulatory authorities and otherwise responding to or addressing developments relating to cross- border personal data transfers may result in substantial costs, require changes to our policies and business practices, require us to engage in additional contractual negotiations, limit our ability to provide certain products in certain jurisdictions, limit our ability to provide certain products to certain customers, or materially adversely affect our business and operating results. ~~Meanwhile~~ **More generally** , ~~the United Kingdom' s~~ **as obligations regarding privacy,** data protection ~~legislation is substantially consistent with the GDPR, and the UK has adopted an extension to the EU- U. S. Data~~

~~Privacy Framework, but it remains to be seen how data transfers to and from the United Kingdom will be regulated and enforced in the longer term. To the extent future United Kingdom data protection requirements diverge significantly from the GDPR, they may result in substantial costs, require changes to our business practices, limit our ability to provide certain products in certain jurisdictions, limit our ability to provide certain products to certain customers, or materially adversely affect our business and operating results. We also expect that there will continue to be new, and amendments to existing, laws, regulations, and industry standards concerning privacy, data protection~~ , and information security **increase** ~~proposed and enacted~~ in the United States and various individual U..... our practices. As data protection compliance complexity ~~grows~~ , we may be required to incur substantial costs to adapt our policies and business practices as well as engage in additional contractual negotiations. Any failure or perceived failure by us to comply with our privacy policies, our privacy- related obligations to customers or other third parties, applicable laws or regulations, or any of our other legal obligations relating to privacy, data protection, or information security may result in governmental investigations or enforcement actions, litigation, claims, or public statements against us by consumer advocacy groups or others and could result in significant liability or cause our customers to lose trust in us, which could cause them to cease or reduce use of our products and otherwise have an adverse effect on our reputation and business. Furthermore, the costs of compliance with, and other burdens imposed by, the laws, regulations, and policies that are applicable to the businesses of our customers may limit the adoption and use of, and reduce the overall demand for, our products. Additionally, if third parties we work with, such as sub- processors, vendors, or developers, violate applicable laws or regulations, contractual obligations, or our policies — or if it is perceived that such violations have occurred — such actual or perceived violations may also have an adverse effect on our business. Further, any significant change to applicable laws, regulations, or industry practices regarding the collection, use, retention, security, disclosure, or other processing of users' content, or regarding the manner in which the express or implied consent of users for the collection, use, retention, disclosure, or other processing of such content is obtained, could increase our costs and require us to modify our network, products, and features, possibly in a material manner, which we may be unable to complete, and may limit our ability to store and process customer data or develop new products and features. We are subject to anti- corruption, anti- bribery, and similar laws, and noncompliance with such laws can subject us to criminal penalties or significant fines and harm our business and reputation. We are subject to the U. S. Foreign Corrupt Practices Act of 1977, the UK Bribery Act 2010, and other anti- corruption, anti- bribery, anti- money laundering, and similar laws in the United States and other countries in which we conduct activities. Anti- corruption and anti- bribery laws, which have been enforced aggressively and are interpreted broadly, prohibit companies and their employees and agents from promising, authorizing, making, or offering improper payments or other benefits to government officials and others in the public sector. We leverage third parties, including channel partners, to sell subscriptions to our products, host many of our co- location facilities for our network, and conduct our business in the United States and abroad. We and these third parties may have direct or indirect interactions with officials and employees of government agencies or state- owned or affiliated entities and we may be held liable for the corrupt or other illegal activities of our business partners and intermediaries, our employees, representatives, contractors, channel partners and agents, even if we do not explicitly authorize such activities. Further, some of our international sales activity occurs, and some of our network infrastructure is located, in parts of the world that are recognized as having a greater potential for business practices that violate anti- corruption, anti- bribery, or similar laws. We cannot assure you that all of our employees and agents, including our channel partners, have complied with, or in the future will comply with, our policies and applicable law. As we continue to increase our international sales and business and expand our network globally, our risks under these laws may increase. The investigation of possible violations of these laws, including internal investigations and compliance reviews that we may conduct from time to time, could have a material adverse effect on our business. Actual or perceived noncompliance with these laws could subject us to investigations, severe criminal or civil sanctions, settlements, prosecution, loss of export privileges, suspension or debarment from U. S. government contracts and other contracts, other enforcement actions, the appointment of a monitor, disgorgement of profits, significant fines, damages, other civil and criminal penalties or injunctions, whistleblower complaints, adverse media coverage and other consequences. Other internal and government investigations, regulatory proceedings, or litigation, including private litigation filed by our stockholders, may also follow as a consequence. Any investigations, actions, or sanctions could materially harm our reputation, business, results of operations, and financial condition. Further, the promulgation of new anti- corruption and anti- bribery laws, rules or regulations or new interpretations of current anti- corruption and anti- bribery laws, rules or regulations could impact the way we do business in other countries, including requiring us to change certain aspects of our business to ensure compliance, which could reduce revenue, increase costs, or subject us to additional liabilities. We may face fines, penalties, or other costs, either directly or vicariously, if any of our partners, resellers, contractors, vendors or other third parties fail to adhere to their compliance obligations under our policies and applicable law. We use a number of partners, resellers, contractors, vendors and other third parties to perform services or act on our behalf in areas like sales, network infrastructure, administration, research, and marketing. It may be the case that one or more of those third parties fail to adhere to our policies or violate applicable federal, state, local, and international laws, including but not limited to, those related to corruption, bribery, economic sanctions, and export / import controls. Despite the significant challenges in asserting and maintaining control and compliance by these third parties, we may be held fully liable for third parties' actions as fully as if they were a direct employee of ours. Such liabilities may create harm to our reputation, inhibit our plans for expansion, or lead to extensive liability either to private parties or government regulators, which could adversely impact our business, results of operations, and financial condition. We may have exposure to greater than anticipated income tax liabilities in the United States and in foreign jurisdictions, requiring us to exercise judgment in determining the applicability of certain tax laws, and this could subject us to potentially adverse tax consequences and adversely impact our results of operations. We operate in a number of tax jurisdictions globally, including in the United States at the federal, state, and local levels, and in many other countries, and plan to continue to expand the scale of our operations in the future. As a result, we are subject to income tax in the United States and

a number of other jurisdictions. In the ordinary course of our global business, we are also subject to various jurisdictional rules regarding the timing and allocation of revenue and expenses, resulting in intercompany transactions and calculations where the ultimate tax determination is uncertain. To the extent taxing authorities may disagree with our positions, it could result in additional taxes, interest, and penalties. Significant judgment is required in determining our worldwide provision for income taxes. Our effective income tax rate may be impacted by changes in the mix of earnings in countries with differing statutory tax rates, changes in non- deductible expenses, changes in excess tax benefits from stock- based compensation, changes in the valuation of deferred tax assets and liabilities and our ability to utilize them, the applicability of withholding taxes, and the effects from acquisitions. Changes in accounting principles, changes in global tax laws, regulations or rates, or changes in taxing jurisdictions' administrative interpretations, decisions, policies, and positions could also impact our provision for income taxes. For example, the United States enacted the Inflation Reduction Act in August 2022, which, among other provisions, implements a 15 % corporate alternative minimum tax on adjusted financial statement income, effective in taxable years beginning after December 31, 2022, and a 1 % excise tax on share repurchases, effective for repurchases made after December 31, 2022, which could include ~~transactions with respect to~~ capped call transactions such as those we entered into in 2020 and 2021. Additionally, the Organization for Economic Cooperation and Development (OECD) published model rules within the OECD / G20 Inclusive Framework on Base Erosion and Profit Shifting (the Inclusive Framework) to address the challenges arising from the digitalization of the global economy. The Inclusive Framework includes provisions related to the taxation of the digital economy and the establishment of a 15 % global minimum tax under Pillar Two. ~~While several~~ **A number of foreign** countries have ~~adopted~~ **enacted**, or intend to **enact, legislation** ~~adopt~~ **adopting** ~~,~~ parts of the Inclusive Framework ~~, some other countries are considering similar changes to their existing tax laws~~. Any of the foregoing changes could have an adverse impact on our results of operations, cash flows, and financial condition. From time to time, we may be subject to income tax audits. While we believe our tax estimates are reasonable and that we have complied with all applicable tax laws, there can be no assurance that a governing tax authority will not have a different interpretation of the law and assess us with additional taxes, including with respect to intercompany transfer pricing. We cannot ensure that the final determination of tax audits or tax disputes will not be different from what is reflected in our historical income tax provisions and accruals and that the outcomes from these continuous examinations will not have an adverse effect on our results of operations. Our results of operations may be harmed if we are required to collect sales and use, value- added, or similar taxes for our products in jurisdictions where we have not historically done so. We are subject to indirect taxes, such as payroll, sales, use, value- added, goods and services, property, and digital services taxes, in both the United States and various foreign jurisdictions. Sales and use, value- added, goods and services, and similar tax laws and rates vary greatly by jurisdiction. Our customers can be located in one jurisdiction, utilize our network and products through our network equipment in a different jurisdiction, and pay us from an account located in a third jurisdiction. This divergence, along with the jurisdiction- by- jurisdiction variance in tax laws, causes significant uncertainty in the tax treatment of our business. There is further uncertainty as to what constitutes sufficient physical presence or nexus for a national, state, or local jurisdiction to levy taxes, fees, and surcharges for sales made over the Internet. There is also uncertainty as to whether our characterization of our network and products as not taxable in certain jurisdictions will be accepted by national, state, and local taxing authorities. In determining our tax filing obligations, management has made judgments regarding whether our activities in a jurisdiction rise to the level of taxability. These judgments may prove inaccurate, and one or more states or countries may seek to impose additional sales, use, or other tax collection obligations on us, including for past sales made by us. We currently face, and in the future may continue to face, non- income tax audits. In the event of an adverse audit outcome, tax authorities could assert that we are obligated to collect additional taxes from our customers, which could exceed our estimated liabilities. A successful assertion by a state, country, or other jurisdiction that we should have been or should be collecting additional sales, use, or other taxes on our network and products could, among other things, result in substantial tax liabilities for past sales, create significant administrative burdens for us, discourage customers from purchasing our network and products, or otherwise harm our business, results of operations, and financial condition. Our ability to use our net operating loss carryforwards and certain other tax attributes may be limited. Under certain circumstances, our income tax obligations may be reduced as a result of our net operating loss carryforwards and other tax attributes. As of December 31, ~~2023~~ **2024**, we had net operating loss carryforwards for U. S. federal and state income tax purposes of $ 1, ~~385~~ **604**. ~~1~~ **0** million and $ ~~756~~ **860**. ~~1~~ **2** million, which will begin to expire in 2029 and ~~2030~~ **2027**, respectively. We had net operating loss carryforwards for U. K. income tax purposes of $ ~~207~~ **209**. ~~2~~ **5** million that can be carried forward indefinitely. Also as of December 31, ~~2023~~ **2024**, we had U. S. federal and state research and development tax credit carryforwards of $ ~~63~~ **73. 4 million and $ 34**. 6 ~~million and $ 29. 8~~ million that will begin to expire in 2029 and 2039, respectively. Utilization of our net operating loss carryforwards and other tax attributes, such as research and development tax credits, may be subject to annual limitations, or could be subject to other limitations on utilization or benefit due to the ownership change limitations provided by Sections 382 and 383 of the Internal Revenue Code of 1986, as amended (the Code), and other similar provisions. Under Sections 382 and 383 of the Code, if a corporation undergoes an " ownership change, " the corporation' s ability to use its pre- change net operating loss carryforwards and other pre- change attributes, such as research tax credits, to offset its post- change income may be limited. In general, an " ownership change " will occur if there is a cumulative change in our ownership by " 5- percent shareholders " that exceeds 50 percentage points over a rolling three- year period. Similar rules may apply under state tax laws. We may have experienced various ownership changes in the past, and we may experience ownership changes in the future as a result of subsequent changes in our stock ownership, some of which may be outside our control. Net operating loss carryforwards and other tax assets could expire before utilization and could be subject to limitations, which could harm our business ~~, revenue,~~ and financial results. It is also possible that federal, state, and non- U. S. tax authorities will enact additional legislation limiting our ability to use our carryforwards, some of which may adversely impact our business. If we are deemed an investment company under the Investment Company Act of 1940, as amended (the 1940 Act), applicable restrictions could make it impractical for us

to continue our business as contemplated and could have a material adverse effect on our business, results of operations, and financial condition. Under the 1940 Act, a company generally will be deemed to be an " investment company " if (1) it is, or holds itself out as being, engaged primarily, or proposes to engage primarily, in the business of investing, reinvesting or trading in securities or (2) it engages, or proposes to engage, in the business of investing, reinvesting, owning, holding or trading in securities and it owns or proposes to acquire investment securities having a value exceeding 40 % of the value of its total assets (exclusive of U. S. government securities and cash items) on an unconsolidated basis. We do not believe that we are an " investment company " under the 1940 Act. We have historically qualified for an exemption from registration under the 1940 Act for " research and development companies " as defined in Rule 3a- 8 promulgated under the 1940 Act. To provide clarity on our investment company status in the longer term, we applied for and, in April 2023, received an order from the SEC stating that we are primarily engaged in a business other than that of investing, reinvesting, owning, holding or trading in securities, and therefore not an investment company, subject to compliance with certain conditions. Notwithstanding the exemptive order, we believe that we have never been an investment company because, among other reasons, we are primarily engaged in the business of a global cloud services provider. We intend to operate our business as described in the exemptive order; however, it is possible that our business will change in the future. If the SEC were to find that the circumstances that gave rise to the issuance of the exemptive order no longer exist, the SEC may revoke the exemptive order. If the exemptive order were revoked or we are unable otherwise to rely on the exemptive order or another applicable exemption, we may be required to institute burdensome requirements to comply with the 1940 Act, which may restrict our activities in a way that could adversely affect our business, results of operations, and financial condition. Risks Related to International Operations Our international operations expose us to significant risks, and failure to manage those risks could materially and adversely impact our business and results of operations. Historically, we have derived a significant portion of our revenue from outside the United States. We derived **49 %,** 48 %, **and** 47 ~~%, and 48~~ % of our revenue from our international customers for the years ended December 31, **2024,** 2023, **and** 2022 ~~, and 2021~~ , respectively. We are continuing to adapt to and develop strategies to address international markets and our growth strategy includes expansion into geographies around the world, but there is no guarantee that such efforts will be successful. In addition, our global network includes co- location facilities located in more than ~~310~~ **335** cities and over ~~120~~ **125** countries worldwide as of December 31, ~~2023~~ **2024** . We expect that our international sales and network activities will continue to grow in the future, as we continue to pursue opportunities in international markets and further grow our network around the world. These international operations will require significant management attention and financial resources and are subject to substantial risks, including: • geopolitical, economic, and social uncertainties, including the potential nationalization of key peering partners by foreign governments or political unrest that affects our ability to continue to work with particular peering partners, potential terrorist activities, military conflict or war, trade policies and sanctions, and the unknown impact of regional or global health crises, or epidemic or pandemic diseases ~~, such as the COVID- 19 pandemic~~ ; • changes in a specific country' s or region' s political or economic conditions **, including the impact of elections and other changes in governments** ; • unexpected costs for the localization of our products, including translation into foreign languages and adaptation for local practices, certifications, and legal and regulatory requirements; • greater difficulty in enforcing contracts and accounts receivable collection, and longer collection periods; • reduced or uncertain protection for intellectual property rights in some countries; • requirements to open local offices or otherwise maintain a local presence in some countries; • greater risk of unexpected changes in regulatory practices, **increased costs due to** tariffs, and tax laws and treaties ~~, including with respect to our business in China~~ ; • increased risk to our local employees of government pressure, including potential threats of prosecution or imprisonment, in connection with enforcement of local legal and regulatory requirements; • greater risk of a failure of foreign employees and channel partners to comply with both U. S. and foreign laws, including antitrust regulations, anti- bribery laws, export and import control laws, and any applicable trade regulations ensuring fair trade practices; • heightened security risks associated with our co- location facilities and related equipment in high- risk countries and the software code and systems access shared with our service providers located in such countries, including in the Hong Kong region as a result of the National Security Law passed in June 2020; • greater security and oversight risks associated with third- party contractors that we use to install and maintain our hardware in co- location facilities in foreign countries and the limited background checks and screening that we can perform on such service providers; • laws and regulations related to privacy, data protection, security requirements, data localization, or content restriction that could pose risks to our intellectual property, increase the cost of doing business in a country, subject us to greater risks of claims and enforcement actions by regulators or others, subject us and our current and potential customers to burdensome requirements, increase the chance that current and potential customers may be unable to use our products or may be required to lessen or alter how they use our products, or create other disadvantages to our business or negative impacts on our results of operations; • increased expenses incurred in establishing and maintaining office space and equipment for our international operations; • greater difficulty in identifying, attracting, and retaining local qualified personnel and the costs and expenses associated with such activities; • differing employment practices and labor relations issues, which may make expansion or contraction of our workforce, or changes in the terms of employment, in such countries more costly and time- consuming and subject us to a greater risk of disputes or litigation; • increased regulatory requirements and litigation risk related to the presence of our physical infrastructure in countries around the world; • difficulties in managing and staffing international offices and increased travel, infrastructure, and legal compliance costs associated with operating multiple international locations; and • fluctuations in exchange rates between the U. S. dollar and foreign currencies in markets where we do business, particularly the United Kingdom, the European Union, and Singapore where we have large offices or a large number of employees and pay employees in local currency. The expansion of our existing international operations and entry into additional international markets will require significant management attention and financial resources. Our failure to successfully manage our international operations and the associated risks could limit the future growth of our business. ~~In particular~~ **For example** , ~~we are exposed to risks in China, which amounts to a significant part of both~~ our ~~short- term and long-~~

~~term revenue growth plans. Our~~ Chinese operations are substantially dependent on our relationship with JD Cloud and due to economic and political challenges in servicing the Chinese market, the loss of this arrangement could have a significant adverse effect on our business and results of operations. Geopolitical events, including the ongoing conflicts **in the Middle East** ~~between Hamas and Israel and between Russia~~ and Ukraine or other areas of geopolitical tension around the world, or any worsening or ~~expanding~~ **expansion** of those conflicts or geopolitical tensions, may increase the likelihood of certain of these risks materializing or heighten their impact on us in affected regions. In addition, heightened use of trade restrictions and sanctions, including tariffs or prohibitions on technology transfers to achieve diplomatic ends could impact our ability to conduct our business as planned. As discussed in greater detail above in our risk factor titled " Our actual or perceived failure to comply with privacy, data protection, information security, and other applicable laws, regulations, and obligations could harm our business, " recent changes in privacy and data protection laws in a number of countries and supranational organizations have created uncertainty around the requirements related to transfers of personal data between jurisdictions, including transfers to the United States. As a result of this uncertainty, our current and potential customers in certain regions may be concerned about whether they are able to transfer personal data to the United States in connection with the usage of our global network and products. If these concerns result in our current and potential customers in those regions reducing their usage of our products, then our results of operations could be adversely impacted. Further, we anticipate needing to identify different transfer mechanisms and / or change our use of certain standard contractual clauses in order to lawfully transfer certain personal data from those regions to the United States. This could result in substantial costs, require changes to our policies and business practices, require us to engage in additional contractual obligations, limit our ability to provide certain products in certain jurisdictions, or materially adversely affect our business and operating results. We are exposed to fluctuations in currency exchange rates, which could negatively affect our results of operations. Substantially all of our sales contracts are denominated in U. S. dollars and, therefore, substantially all of our revenue is not subject to foreign currency risk. However, a strengthening of the U. S. dollar has increased and may continue to increase the real cost of our products to our customers outside of the United States, which could reduce demand for our products or cause us to discount our products, which could adversely affect our financial condition and results of operations. As our international operations expand, an increasing portion of our operating expenses is incurred outside the United States and is denominated in foreign currencies, such as the British Pound, Euro, and Singapore Dollar. In addition, in the future we may begin to generally allow customers in some countries outside the United States to pay us for our products in the currencies of those countries. Accordingly, our revenue and operating expenses may be increasingly subject to fluctuations due to changes in foreign currency exchange rates. As we continue to expand our international operations, we may become more exposed to foreign currency risk or remeasurement risk. ~~If~~ **In the second quarter of 2024, we initiated a foreign exchange hedging program that uses derivative instruments to lessen the effects of currency fluctuations on certain of our non- U. S. dollar denominated currency exposures. However, our hedging instruments may not successfully mitigate losses caused by currency fluctuations, and our hedging positions may be partial or may not exist at all in the future. In addition, the use of hedging instruments may bring additional risks if we are unable to arrange effective hedges with such instruments or if we are unable to forecast hedged exposures precisely. While we have in the past, and may in the future, choose to enter into additional transactions to hedge portions of our foreign exchange exposures, it is impossible to predict or eliminate the effects of foreign exchange rate exposure, and if** we become more exposed to currency fluctuations and are not able to successfully hedge against the risks associated with currency fluctuations, our results of operations could be materially and adversely affected. Our business could be adversely impacted by the decision of foreign governments, Internet service providers, or others, to block transmission from Cloudflare IP addresses or domains in order to enforce certain Internet content blocking efforts. Some of our security products involve making origin IP addresses and other operational assets of our customers more difficult for cyber attackers to target. The evolving design of our network and products may create challenges for various organizations, including governments, that seek to block certain content based on IP address " block lists " or other mechanisms. This problem is exacerbated by the fact that a single Cloudflare IP address may be used for a number of Internet properties, and the Cloudflare IP used for any one Internet property may change over time. This means that efforts by ISPs to block a single domain name may end up blocking a number of other domains or content. If these challenges become too difficult for those organizations to overcome, they could make the decision to block content in an overbroad manner or block completely websites and other Internet properties that are using our network and / or transmitted using known Cloudflare IP addresses. Some of these blocking efforts would be out of our control once they have been put in place and may limit our ability to provide our products on a fully global basis, which could reduce demand for our products among current or potential customers that are focused on the impacted regions or could otherwise adversely impact our business, results of operations, and financial condition. Our network presence within China is dependent upon our commercial relationship with JD Cloud, and any detrimental changes in, or the termination of, that relationship could jeopardize our ability to offer an integrated global network that includes China. We believe our offering of an integrated global network that includes facilities in China is important to our existing and potential future customers. Our ability to continue to offer an integrated network presence that includes China currently is dependent on our commercial relationship with JD Cloud. Regulation of Internet infrastructure and traffic by the Chinese government creates challenges to the peering of Chinese and non- Chinese networks. We have a strategic agreement with JD Cloud to provide solutions that accommodate the requirements imposed by Chinese regulations through JD Cloud' s development and operation of facilities in China that are included as part of our network. Our ~~original~~ **current** agreement with JD Cloud ~~was announced in 2020 and was set to expire in April 2023. A new agreement~~ , **which** ~~extending the relationship, was executed in April 2023 and~~ is set to expire in March 2026 **,** ~~. The new agreement~~ contains economic terms that are less favorable to us than the terms of the original agreement **with JD Cloud that expired in 2023** . Consistent with the original agreement, our ~~new~~ **current** agreement with JD Cloud is subject to earlier termination by either party under certain circumstances such as the other party' s material breach and can be terminated by JD

Cloud under certain circumstances if necessary Chinese governmental approvals are revoked or become limited or impaired or if public law or regulatory action by the Chinese or U. S. government expressly prohibits or materially restricts the collaboration contemplated by the agreement. The risk of such an early termination event may have increased during the current environment of economic trade negotiations and tensions between the Chinese and U. S. governments. Our customers that use our network presence in China through our JD Cloud commercial relationship are subject to Chinese laws and regulations of Internet infrastructure, traffic, and content. Under our agreement with JD Cloud, in some circumstances, these customers' use of our Chinese network presence can be terminated if they violate these laws and regulations. The removal of our customers from our Chinese network presence could result in these customers deciding to terminate their overall relationship with us. In addition, any adverse publicity associated with the removal of some or all of our customers from our Chinese network presence as a result of the application of Chinese laws and regulations could cause us to experience adverse reputational and business consequences. If our commercial relationship with JD Cloud is terminated, identifying an alternative solution in China could be difficult, time-consuming, and expensive. Even if an alternative solution is identified, we cannot be certain that the economic terms or performance of any such alternative arrangement will be comparable to our existing relationship with JD Cloud, which could materially negatively impact our financial results and customer satisfaction with such alternative arrangement. A lack of network presence in China would represent a significant loss of utility to many of our customers and could materially harm our business, financial condition, or results of operations. We are subject to governmental trade sanctions laws, and export and import controls, that could impair our ability to compete in international markets and subject us to liability if we are not in full compliance with applicable laws. Our business activities are subject to various economic and trade sanctions regulations administered by the U. S. Department of the Treasury' s Office of Foreign Assets Control (OFAC) and U. S. export control and similar foreign laws and regulations, including the U. S. Department of Commerce' s Export Administration Regulations (EAR). We incorporate encryption technology into certain of our products, and the encryption products and the underlying technology may be exported outside the United States only with the required export authorizations, including by license, a license exception, or other appropriate government authorizations, including the filing of classification requests or self- classification reports. Further, the U. S. economic sanctions laws and export control laws include restrictions or prohibitions on the sale or supply of most products and services to U. S. embargoed or sanctioned countries, governments, persons, and entities. Even though we take precautions and have implemented policies and practices to assist in compliance, there is a risk that we may not be in full compliance with these laws. In 2019, we learned that we may have failed to comply with certain U. S. export- related filing and reporting requirements and may have submitted incorrect information to the U. S. government in connection with certain hardware exports. Upon learning of these potential violations and associated export control requirements, we promptly initiated a voluntary internal review and are taking remedial measures to prevent similar export control anomalies from occurring in the future. In May 2019, we submitted an initial voluntary self- disclosure to the Bureau of Industry and Security regarding potential violations of EAR and a voluntary self- disclosure to the Census Bureau regarding potential violations of the Foreign Trade Regulations. In July 2019, we filed the full and complete voluntary self- disclosures. The voluntary self-disclosure to the Census Bureau was completed with no penalties in November 2019. The voluntary self- disclosure to the Bureau of Industry and Security was completed with no penalties in June 2020. In May 2019, we submitted an initial voluntary self- disclosure to OFAC related to our non- compliance with certain economic and trade sanctions programs, and we filed the full and complete voluntary self- disclosure to OFAC in July 2019. Specifically, we identified that our products were used by, or for the benefit of, certain individuals and entities included in OFAC' s Specially Designated Nationals and Blocked Persons List, including entities identified in OFAC' s counter- terrorism and counter- narcotics trafficking sanctions programs and individuals or entities affiliated with governments currently subject to comprehensive U. S. sanctions or located in regions subject to comprehensive sanctions. A small number of these parties made payments to us in connection with their use of our products. The voluntary self- disclosure, which we may supplement as appropriate, remains under an ongoing review by OFAC. Although we have implemented, and are working to implement additional controls and screening tools designed to prevent similar activity from occurring in the future, there is no guarantee that we will not inadvertently provide our products to additional individuals, entities, or governments prohibited by U. S. sanctions in the future. Additionally, we currently provide products to certain OFAC- sanctioned regions based upon general licenses issued by OFAC to engage in such activity. We continue to review the OFAC sanctions and our practices to verify compliance. These efforts related to export controls and OFAC sanctions could result in negative consequences for us, including costs related to government investigations, financial penalties and harm to our reputation. The impact on us related to these matters could be substantial. In addition, various countries regulate the import of certain technologies and have enacted or could enact laws that could limit our ability to provide our products and operate our network or could limit our customers' ability to access or use our network and products in those countries. If we are found to have violated the U. S. or foreign laws and regulations, we and certain of our employees could be subject to civil or criminal penalties, including the possible loss of export privileges and fines. We may be materially and adversely affected through penalties, reputational harm, loss of access to certain markets, loss of customers, or otherwise. Obtaining the necessary authorizations, including any required license, for a particular transaction may be time- consuming, is not guaranteed, and may result in the delay or loss of sales opportunities. In addition, changes in our network, products, or screening process, or changes in export, sanctions, and import laws, could delay the introduction and sale of subscriptions to our products in international markets, prevent customers in certain countries from accessing our network and products or, in some cases, prevent the provision of our network and products to certain countries, governments, persons, or entities altogether. Any decrease in our ability to sell our products could materially and adversely affect our business, results of operations, and financial condition. Risks Related to Intellectual Property We are currently, and may be in the future, party to intellectual property rights claims and other litigation matters that, if resolved adversely, could have a material impact on our business, results of operations, or financial condition. We own a large number of 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 rights. 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. In addition, a number of companies in our industry hold a large number of patents and also protect their copyright, trade secret, trademark, and other intellectual property rights, and companies in the networking and security industry frequently enter into litigation based on allegations of patent infringement or other violations of intellectual property rights. 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 intellectual property, our business practices, and our products. For example, we are a defendant in lawsuits, both in the United States and abroad, seeking injunctive relief and / or damages against us based on claims of alleged patent infringement and claims of alleged copyright infringement through content on our customers' websites. **Courts in some countries have found that we may be held liable in certain circumstances for damages arising from infringement on a customer' s website or directed us to take action by removing access to content of certain websites and other Internet properties on our network.** We may also be subject to governmental and other regulatory investigations from time to time. The costs of supporting litigation and dispute resolution proceedings are considerable, and there can be no assurances that a favorable outcome will be obtained. Disputes, whether or not favorably resolved, also may generate negative publicity and damage our reputation. 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. 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, results of operations, and financial condition could be materially and adversely affected as a result. Indemnity provisions in various agreements potentially expose us to substantial liability for intellectual property infringement and other losses. Our agreements with certain of our customers or other third parties may include indemnification or other provisions under which we agree to indemnify or otherwise be liable to them for losses suffered or incurred as a result of claims of intellectual property infringement, damages caused by us to property or persons, or other liabilities relating to or arising from the use of our network and products or other acts or omissions. The term of these contractual provisions often survives termination or expiration of the applicable agreement. We have in the past been sued on the basis of alleged violation of intellectual property rights in the form of patents and trade secrets. Although we were successful in defending the claims to date, as we continue to grow, the possibility of these and other intellectual property rights claims against us may increase. For any intellectual property rights indemnification claim against us or our customers, we may incur significant legal expenses and have to pay damages, pay license fees and / or stop using technology found to be in violation of the third party' s rights. Large indemnity payments could harm our business, results of operations, and financial condition. We may also have to seek a license for the disputed technology, but such a license may not be available on reasonable terms, if at all, and may significantly increase our operating expenses or may require us to restrict our business activities and limit our ability to deliver certain products. As a result, we may also be required to develop alternative non- infringing technology, which could require significant effort and expense and / or cause us to alter our network or products, which could negatively affect our business. From time to time, customers require us to indemnify or otherwise be liable to them for breach of confidentiality, violation of applicable law, or failure to implement adequate security measures with respect to their data stored, transmitted, or accessed using our network and products. Our standard Enterprise plan agreements provide limited indemnification to our customers based on third- party claims related to our violation of intellectual property rights, and some of our Enterprise plan agreements offer indemnification for claims beyond that scope. The existence of such a dispute may have adverse effects on our customer relationship and reputation and we may still incur substantial liability related to them. Any assertions by a third party, whether or not successful, with respect to such indemnification obligations could subject us to costly and time- consuming litigation, expensive remediation and licenses, divert management attention and financial resources, harm our relationship with that customer and other current and prospective customers, reduce demand for our products, and harm our brand, business, results of operations, and financial condition. Our failure to protect our intellectual property rights and proprietary information could diminish our brand and other intangible assets. We rely and expect to continue to rely on a combination of patent, patent licenses, trade secret, domain name protection, trademarks, copyrights, and confidentiality and license agreements with our employees, consultants, and third parties in order to protect our intellectual property rights and proprietary information. As of December 31, ~~2023~~ **2024** , we had ~~290~~ **334** issued patents and ~~67~~ **72** pending patent applications in the United States and abroad. However, third parties may knowingly or unknowingly infringe our intellectual property rights. Third parties may challenge our intellectual property rights, pending and future patent, trademark, and copyright applications may not be approved, and we may not be able to prevent infringement, misappropriation, or violations of our intellectual property rights without incurring substantial expense. We have also devoted substantial resources to the development of our proprietary technologies and related processes, and we provide access to these technologies and processes to certain of our vendors and partners, including JD Cloud with respect to the facilities included within our network in China. We must protect this proprietary information in order to realize commercial benefit from our investment. In order to protect our proprietary technologies and processes, we rely in part on trade secret laws and confidentiality agreements with our employees, contractors, 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. Further, errors made by our employees or contractors in utilizing artificial intelligence or machine learning in our products or in the operation of our business could result in proprietary or other confidential information being exposed externally. In addition, others may independently discover our

trade secrets or develop similar technologies and processes, in which case we would not be able to assert trade secret rights against them. Laws in certain jurisdictions may afford little or no trade secret protection, and any changes in, or unexpected interpretations of, the intellectual property laws in any country in which we operate may compromise our ability to enforce our intellectual property rights. We may not be effective in policing unauthorized use of our intellectual property rights, and even if we do detect violations, costly and time- consuming litigation could be necessary to enforce and determine the scope of our proprietary rights, and any such litigation could be unsuccessful, lead to the invalidation of our proprietary rights, or lead to counterclaims by other parties against us. If the protection of our proprietary rights is inadequate to prevent use or appropriation by third parties, the value of our network and products, brand, and other intangible assets may be diminished and competitors may be able to more effectively replicate our network and products and their features. Any of these events could materially and adversely affect our business, results of operations, and financial condition. We depend and rely upon software and technologies licensed from third parties to operate our business, and interruptions or the unavailability of these technologies may adversely affect our products, network, business, and results of operations. We rely on software, services, and other technology from third parties that we incorporate into, or integrate with, our network and products. We also rely on software, services, and other technology from third parties in order to operate critical functions of our business, including enterprise resource planning and customer relationship management services. If the software, services, or other technology we rely on become unavailable due to extended outages, the third- party provider disabling our access, expiration or termination of licenses, or because they are otherwise no longer available on commercially reasonable terms, 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 obtained or replacements are developed, all of which could adversely affect our business. If we are unable to license necessary technology from third parties now or in the future, we may be forced to acquire or develop alternative technology, which we may be unable to do in a commercially feasible manner or at all, and we may be required to use alternative technology of lower quality or performance. This could limit and delay our ability to offer new or competitive products and increase our costs of production. As a result, our business and results of operations could be significantly harmed. We cannot be certain that those from whom we license software and other technology are not infringing the intellectual property rights of third parties or have sufficient rights to the licensed intellectual property in all jurisdictions in which we may sell our products. Accordingly, our use of this intellectual property may expose us to third- party claims of infringement. In addition, many licenses are non-exclusive and may not prevent our competitors from licensing the same technology on equivalent or more favorable terms. Some of our technology incorporates " open source " software, we license some of our software through open source projects and we voluntarily make available some of our software on an open source basis, which could negatively affect our ability to sell our products, subject us to possible litigation, and be used by other companies to compete against us. Our network and products incorporate software licensed under open source licenses, including open source software included in software we receive from third- party commercial software vendors. Use of open source software may entail greater risks than use of third-party commercial software, as open source licensors generally do not provide support, updates, or warranties, or other contractual protections regarding infringement claims or the quality of the software. In addition, the wide availability of source code incorporated in our products could allow hostile parties to more easily identify security vulnerabilities in our network and products. The terms of some open source licenses may provide that under certain conditions we could be required to release the source code of our proprietary software, and to make our proprietary software available under open source licenses, including authorizing further modification and redistribution. In the event that certain portions of our proprietary software are determined to be subject to such requirements by an open source license, we could be required to publicly release the affected portions of our source code, re- engineer all or a portion of our network or applicable products, or otherwise be limited in the licensing of our products, each of which provide an advantage to our competitors or other entrants to the market, create security vulnerabilities in our products, and could reduce or eliminate the value of our products. Because the terms of open source licenses are novel and have not been widely interpreted by courts, we could be subject to lawsuits by parties claiming ownership of what we believe to be open source software or by third parties seeking to enforce the terms of open source licenses against us in a manner we do not anticipate. In addition, we voluntarily make available certain portions of our software on an open source basis to the public and such software could then be used by other companies to compete against us. Any unanticipated disclosure of, or litigation regarding, our source code and any open source software incorporated into our source code could result in adverse judgments and liabilities, require us to reengineer all or a portion of our network and products, limit the marketing of our products, provide an advantage to our competitors or other entrants to the market, create new security vulnerabilities or highlight existing security vulnerabilities in our network and products, and reduce or eliminate the value of our network and products. We cannot assure you that our processes for controlling our use of open source software in our network and products will be effective. 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 may 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: • price and volume fluctuations in the overall stock market from time to time; • volatility in the trading prices and trading volumes of technology stocks or high growth companies; • changes in operating performance and stock market valuations of other technology or high growth companies generally, or those in our industry in particular; • sales of shares of our Class A common stock and Class B common stock by us or our stockholders; • issuance of shares of our Class A common stock and Class B common stock, whether in connection with an acquisition, upon conversion of some or all of our outstanding 2026 Notes, or in connection with employee equity awards; • failure of securities analysts to maintain coverage of us, changes in financial estimates or share price targets by securities analysts who follow our company, or our failure to meet these estimates or the expectations of investors; • the financial guidance we may provide to the public, any changes in such

guidance, or our failure to meet such guidance; • announcements by us or our competitors of new products, features, or services or any delays in our general release of products we previously announced as being in development or beta testing; • 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; • investments we may make in equity that is, or may become, publicly held, and volatility we may experience due to changes in the market prices of such equity investments; • 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; • actual or perceived network or data security breaches or other network or data security incidents, including any network or product outages or failures; • announced or completed acquisitions of businesses, products, services, or technologies by us or our competitors; • failures or alleged failures to comply with laws or regulations applicable to our business; • new laws or regulations or new amendments to, or interpretations of, existing laws or regulations applicable to our business; • changes in accounting standards, policies, guidelines, interpretations, or principles; • any departure of one of our co- founders from our company or any other significant change in our management; and • general economic conditions and slow or negative growth of our markets, including inflation and related changes in monetary policy, rising interest rates, volatile energy prices, and other impacts of the ~~Hamas- Israel~~ **conflicts in the Middle East** and ~~Russia-~~ Ukraine ~~conflicts~~, or other areas of geopolitical tension around the world, or any worsening or ~~expanding~~ **expansion** of those conflicts or geopolitical tensions. In addition, in the past, following periods of volatility in the overall market and the market price of a particular company' s securities, securities class action litigation has often been instituted against these companies. This litigation, if instituted against us, could result in substantial costs and a diversion of our management' s attention and resources. The dual class structure of our common stock has the effect of concentrating voting control with those stockholders who held our capital stock prior to the completion of our initial public offering, and it may depress the trading price of our Class A common stock. Our Class B common stock has 10 votes per share and our Class A common stock has one vote per share. As of December 31, ~~2023~~ **2024**, our directors, executive officers, and holders of more than 5 % of our common stock, and their respective affiliates, held in the aggregate ~~75~~ **73**. ~~4~~ **5** % of the voting power of our capital stock, with our co- founders together holding approximately ~~54~~ **52**. 8 % of the voting power of our capital stock. Because of the ten- to- one voting ratio between our Class B and Class A common stock, the holders of our Class B common stock collectively continue to control a majority of the combined voting power of our common stock and therefore are able to control all matters submitted to our stockholders for approval. This concentrated control will limit or preclude the ability of holders of Class A common stock to influence corporate matters for the foreseeable future, including the election of directors, amendments of our organizational documents, and any merger, consolidation, sale of all or substantially all of our assets, or other major corporate transaction requiring stockholder approval. In addition, this may prevent or discourage unsolicited acquisition proposals or offers for our capital stock that you may feel are in your best interest as one of our stockholders. Future transfers by holders of shares of Class B common stock and the cessation of employment by holders of our Class B common stock generally result in those shares converting to Class A common stock, subject to limited exceptions, such as certain transfers effected for estate planning purposes and transfers between related entities. The conversion of Class B common stock to Class A common stock will have the effect, over time, of increasing the relative voting power of those individual holders of Class B common stock who retain their shares in the long- term. In July 2017, FTSE Russell announced that it would cease to include most newly public companies utilizing dual or multi- class capital structures in its indices, including the Russell 1000, Russell 2000, and Russell 3000. Under the announced policies, our multi- class capital structure in some cases may make us ineligible for inclusion in some or all of these indices, and as a result, mutual funds, exchange- traded funds, and other investment vehicles that attempt to passively track these indices may not invest in our stock if we are not included. It is unclear what effect, if any, these policies have on the valuations of publicly traded companies excluded from the indices, but it is possible that they may depress these valuations compared to those of other similar companies that are included. Previously, Standard & Poor' s also excluded companies utilizing dual or multi- class capital structures from its indices, including the S & P 500, the S & P MidCap 400, and the S & P SmallCap 600, which S & P indices together make up the S & P Composite 1500. However, in April 2023, it reversed this policy and announced that companies with dual or multi- class capital structures will again be eligible for inclusion on its indices. We cannot be sure that such policy, or the policies of other indices, will not change further and make us ineligible for inclusion on the S & P Composite 1500, or other indices, in the future. Substantial future sales could depress the market price of our Class A common stock. The market price of our Class A common stock could decline as a result of sales of a large number of shares of such stock, and the perception that these sales could occur may also depress the market price of our Class A common stock. **We** ~~Under our investors' rights agreement, certain stockholders can require us to register shares owned by them for public sale in the United States. In addition, we~~ file registration statements to register shares reserved for future issuance under our equity compensation plans. As a result, subject to the satisfaction of applicable exercise periods, the shares issued upon exercise of outstanding stock options or upon settlement of outstanding RSU awards are available for immediate resale in the United States in the open market. Sales of our shares may make it more difficult for us to sell equity securities in the future at a time and at a price that we deem appropriate. These sales also could 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. We have broad discretion over the use of the net proceeds from our financing activities, and we may not use them effectively. We cannot specify with any certainty the particular uses of the net proceeds that we received from our prior financing activities, including from the issuances of the **2025** Notes ~~in~~ **and the** ~~2020~~ **2026 Notes** ~~and 2021~~, and our management has broad discretion in the application of the net proceeds. The failure by our management to apply these proceeds effectively could adversely affect our business, results of operations, and financial condition. Pending their use, we may invest our proceeds in a manner that does not produce income or that loses value. Our investments may not yield a favorable return to

our investors and may negatively impact the price of our Class A common stock. Delaware law and provisions in our amended and restated certificate of incorporation and amended and restated bylaws could make a merger, tender offer, or proxy contest difficult, thereby depressing the market price of our Class A common stock. Our status as a Delaware corporation and the anti- takeover provisions of the Delaware General Corporation Law may discourage, delay, or prevent a change in control by prohibiting us from engaging in a business combination with an interested stockholder for a period of three years after the person becomes an interested stockholder, even if a change of control would be beneficial to our existing stockholders. In addition, our amended and restated certificate of incorporation and amended and restated bylaws contain provisions that may make the acquisition of our company more difficult, including the following: • our dual- class common stock structure, which provides Mr. Prince and Ms. Zatlyn with the ability to significantly influence the outcome of matters requiring stockholder approval, even if they own significantly less than a majority of the shares of our outstanding Class A common stock and Class B common stock; • our Board of Directors is classified into three classes of directors with staggered three- year terms and directors are only able to be removed from office for cause; • vacancies on our Board of Directors will be able to be filled only by our Board of Directors and not by stockholders; • only the Chair of our Board of Directors, our Chief Executive Officer, or a majority of our entire Board of Directors are authorized to call a special meeting of stockholders; • certain litigation against us can only be brought in Delaware; • our amended and restated certificate of incorporation authorizes undesignated preferred stock, the terms of which may be established and shares of which may be issued, without the approval of the holders of Class A common stock; • advance notice procedures apply for stockholders to nominate candidates for election as directors or to bring matters before an annual meeting of stockholders; • our stockholders will only be able to take action at a meeting of stockholders and not by written consent; and • any amendment of the above anti- takeover provisions in our amended and restated certificate of incorporation or amended and restated bylaws will require the approval of two- thirds of the combined vote of our then- outstanding shares of Class A common stock and Class B common stock. These anti- takeover defenses could discourage, delay, or prevent a transaction involving a change in control of our company. These provisions could also discourage proxy contests and make it more difficult for stockholders to elect directors of their choosing and to cause us to take other corporate actions they desire, any of which, under certain circumstances, could limit the opportunity for our stockholders to receive a premium for their shares of our capital stock, and could also affect the price that some investors are willing to pay for our Class A common stock. Our amended and restated bylaws provide that the Court of Chancery of the State of Delaware and the federal district courts of the United States will be the exclusive forums for substantially all 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 bylaws provide that the Court of Chancery of the State of Delaware is 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, stockholders, officers, or other employees to us or our stockholders; (iii) any action arising pursuant to any provision of the Delaware General Corporation Law, our amended and restated certificate of incorporation or our 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. Our amended and restated bylaws further provide that the U. S. federal district courts will be the sole and exclusive forum for resolving any complaint asserting a cause of action arising under the Securities Act, against any person in connection with any offering of our securities, including any auditor, underwriter, expert, control person, or other defendant. Any person or entity purchasing, holding, or otherwise acquiring any interest in any of our securities shall be deemed to have notice of and consented to this provision. 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 the exclusive- forum provision in our amended and restated bylaws to be inapplicable or unenforceable in an action, we may incur additional costs associated with resolving the dispute in other jurisdictions, which could harm our results of operations. Our Class A common stock market price and trading volume could decline if equity 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 equity 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 few securities analysts commence coverage of us, or if one or more of these 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. An active trading market for our Class A common stock may not be sustained. Our Class A common stock is listed on the NYSE under the symbol " NET. " However, we cannot assure you of the likelihood that an active trading market for our Class A common stock will be maintained, the liquidity of any trading market, your ability to sell your shares of our Class A common stock when desired, or the prices that you may obtain for your shares. 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 gains on their investment. Risks Related to our ~~Outstanding Convertible Senior Notes~~ **Indebtedness Our credit agreement and any other credit or similar agreements into which we may enter in the future may restrict our operations, particularly our ability to respond to changes or to take certain actions regarding our business. Our credit agreement, which provides for the Revolving Credit Facility, contains a number of negative**

**covenants that impose operating and financial restrictions on us and limit our ability to engage in acts that may be in our long- term interest, including covenants limiting our ability to, among other things, incur debt, grant liens, undergo certain fundamental changes, dispose of assets, make certain restricted payments and prepayments, enter into restrictive agreements, enter into transactions with affiliates, make investments, and amend certain agreements relating to debt, in each case, subject to limitations and exceptions set forth in the credit agreement. The credit agreement also requires us to maintain compliance with a maximum consolidated net leverage ratio and a minimum interest coverage ratio, in each case, calculated in accordance with the terms of the credit agreement. The credit agreement contains various customary events of default that include, among others, non- payment of principal, interest or fees, breach of covenants, inaccuracy of representations and warranties, cross defaults to certain other indebtedness, bankruptcy and insolvency events, material judgments, and events constituting a change of control, subject to thresholds and cure periods as set forth in the credit agreement. Upon the occurrence and during the continuance of an event of default, the lenders may terminate their commitments and accelerate our obligations under the credit agreement and may exercise certain other rights and remedies provided for under the credit agreement, the other loan documents and applicable law. In the event that our lenders accelerated the repayment of the borrowings under the credit agreement, we may not have sufficient assets to repay that indebtedness. As a result of these restrictions, we may be limited in how we conduct business, unable to raise additional debt or equity financing to operate during general economic or business downturns, or unable to compete effectively or to take advantage of new business opportunities. In addition, we may enter into other credit agreements or other debt arrangements from time to time which contain similar or more extensive negative covenants and events of default, in which case we may face similar or additional limitations as a result of the terms of those credit agreements or other debt arrangements.** Repaying and servicing our existing and future debt, including our 2026 Notes **and our Revolving Credit Facility** , may require a significant amount of cash, and we may not have sufficient cash flow from our business to pay our indebtedness. In August 2021, we issued $ 1, 293. 8 million in aggregate principal amount of the 2026 Notes ~~. As~~ **and, as** of December 31, ~~2023~~ **2024** , the remaining aggregate principal amount was $ 1, 293. 8 million ~~of the~~ **. In addition, in May** ~~2026~~ **2024** ~~Notes~~ **, we entered into a senior secured credit agreement with a $ 400 million Revolving Credit Facility** . Our ability to make scheduled payments of the principal of, or to refinance our indebtedness, including the 2026 Notes **and any borrowings under our Revolving Credit Facility** , depends on our future performance, which is subject to economic, financial, competitive, and other factors beyond our control. Our business may not generate cash flow from operations in the future sufficient to service our debt and make necessary capital expenditures. If we are unable to generate such cash flow, we may be required to adopt one or more alternatives, such as selling assets, restructuring debt, or obtaining additional debt financing or equity capital on terms that may be onerous or highly dilutive. Our ability to refinance any future indebtedness will depend on the capital markets and our financial condition at such time. We may not be able to engage in any of these activities or engage in these activities on desirable terms, which could result in a default on our debt obligations. In addition, **the credit agreement for our Revolving Credit Facility contains restrictive covenants that limit us, and** any of our future debt agreements may contain restrictive covenants that may **limit or** prohibit us **, in each case** from adopting any of these alternatives. Our failure to comply with these covenants could result in an event of default which, if not cured or waived, could result in the acceleration of our debt. In addition, our indebtedness, combined with our other financial obligations and contractual commitments, could have other important consequences. For example, it could: • make us more vulnerable to adverse changes in general U. S. and worldwide economic, industry, and competitive conditions and adverse changes in government regulation; • limit our flexibility in planning for, or reacting to, changes in our business and our industry; • place us at a disadvantage compared to our competitors who have less debt; • limit our ability to borrow additional amounts to fund acquisitions, for working capital, and for other general corporate purposes; and • make an acquisition of our company less attractive or more difficult. Any of these factors could harm our business, results of operations, and financial condition. In addition, if we incur additional indebtedness, the risks related to our business and our ability to service or repay our indebtedness would increase. We may not have the ability to raise the funds necessary for cash settlement upon conversion of the 2026 Notes or to repurchase the 2026 Notes for cash upon a fundamental change, and our future debt may contain limitations on our ability to pay cash upon conversion of the 2026 Notes or to repurchase the 2026 Notes. Holders of the 2026 Notes have the right to require us to repurchase their 2026 Notes upon the occurrence of a fundamental change (which is defined in the 2026 Indenture) at a repurchase price equal to 100 % of the principal amount of such 2026 Notes to be repurchased, plus accrued and unpaid interest, if any, to, but excluding, the fundamental change repurchase date for such series of 2026 Notes. In addition, upon conversion of the 2026 Notes, unless we elect to deliver solely shares of our Class A common stock to settle such conversion (other than paying cash in lieu of delivering any fractional share), we will be required to make cash payments in respect of the 2026 Notes being converted. However, we may not have enough available cash or be able to obtain financing at the time we are required to make repurchases of the 2026 Notes surrendered or 2026 Notes being converted. In addition, our ability to repurchase the 2026 Notes or to pay cash upon conversions of the 2026 Notes may be limited by law, by regulatory authority or by agreements governing our future indebtedness. Our failure to repurchase the 2026 Notes at a time when the repurchase is required by the 2026 Indenture or to pay any cash payable on future conversions of the 2026 Notes as required by the 2026 Indenture would constitute a default. A default under the 2026 Indenture or the occurrence of a fundamental change under the 2026 Notes could also lead to a default under agreements governing our future indebtedness. If the repayment of the related indebtedness were to be accelerated after any applicable notice or grace periods, we may not have sufficient funds to repay the indebtedness and repurchase the 2026 Notes or make cash payments upon conversions thereof in accordance with the terms of the 2026 Indenture. Any failure by us to repay the indebtedness and repurchase the 2026 Notes or make cash payments upon conversions thereof, in each case, when required to do so pursuant to the terms of the 2026 Indenture could harm our business, results of operations, and financial condition. The conditional conversion feature of the 2026 Notes, when triggered, may adversely affect our financial condition

and operating results. If the conditional conversion feature of the 2026 Notes is triggered, holders of the 2026 Notes are entitled to convert their 2026 Notes at any time during specified periods at their option. If one or more holders elect to convert their 2026 Notes, unless we elect to satisfy our conversion obligation by delivering solely shares of our Class A common stock (other than paying cash in lieu of delivering any fractional share), we would be required to settle a portion or all of our conversion obligation through the payment of cash, which could adversely affect our liquidity. In addition, we could be required under applicable accounting rules to reclassify all or a portion of the outstanding principal of the 2026 Notes as a current rather than long- term liability, which would result in a material reduction of our net working capital. Transactions relating to the **2026** Notes may affect the value of our Class A common stock. The conversion of some or all of the 2026 Notes would dilute the ownership interests of our existing stockholders to the extent we satisfy our conversion obligation by delivering shares of our Class A common stock upon any conversion of the 2026 Notes. The 2026 Notes may become convertible at the option of their holders under certain circumstances set forth in the 2026 Indenture. If holders of the 2026 Notes elect to convert their 2026 Notes, we may settle our conversion obligation by delivering to them a significant number of shares of our Class A common stock, which would cause dilution to our existing stockholders. In addition, from time to time, we may enter into certain exchange transactions with respect to the 2026 Notes which may also cause dilution to our existing stockholders. For example, in August 2021, we entered into privately- negotiated exchange agreements with certain holders of the 2025 Notes for the exchange of approximately $ 400. 7 million in cash and approximately 7. 6 million shares of our Class A common stock for $ 400. 0 million in aggregate principal amount of the 2025 Notes. In addition, during the year ended December 31, 2023, we settled conversions of approximately $ 35. 4 million aggregate principal amount of the 2025 Notes for approximately 0. 5 million shares of our Class A common stock. These conversions were exercised by the holders of the 2025 Notes in connection with our issuance of a redemption notice. In connection with the pricing of **the 2026** ~~each series of~~ Notes, we entered into privately negotiated capped call transactions with the applicable option counterparties. The capped call transactions are expected generally to reduce the potential dilution upon conversion of the **2026** ~~applicable series of~~ Notes and / or offset any cash payments we are required to make in excess of the principal amount of such converted **2026** Notes, as the case may be, with such reduction and / or offset subject to a cap. In connection with establishing their initial hedges of the capped call transactions, the applicable option counterparties or their respective affiliates entered into various derivative transactions with respect to our Class A common stock and / or purchased shares of our Class A common stock concurrently with or shortly after the pricing of the **2026** ~~applicable series of~~ Notes. From time to time, the option counterparties or their respective affiliates may modify their hedge positions by entering into or unwinding various derivatives with respect to our Class A common stock and / or purchasing or selling our Class A common stock or other securities of ours in secondary market transactions prior to the maturity of the **2026** ~~applicable series of~~ Notes (and are likely to do so following any conversion, repurchase, or redemption of ~~such~~ **the 2026** Notes, to the extent we exercise the relevant election under the applicable capped call transactions). This activity could also cause a decrease and / or increased volatility in the market price of our Class A common stock. We are subject to counterparty risk with respect to the capped call transactions. The option counterparties are financial institutions, and we will be subject to the risk that any or all of them might default under the capped call transactions. Our exposure to the credit risk of the option counterparties will not be secured by any collateral. Past macroeconomic conditions have resulted in the actual or perceived failure or financial difficulties of many financial institutions, including the failures of Silicon Valley Bank and Signature Bank, and the UBS takeover of Credit Suisse. If an option counterparty becomes subject to insolvency proceedings, we will become an unsecured creditor in those proceedings with a claim equal to our exposure at that time under the capped call transactions with such option counterparty. Our exposure will depend on many factors but, generally, an increase in our exposure will be correlated to an increase in the market price and in the volatility of our Class A common stock. In addition, upon a default by an option counterparty, we may suffer adverse tax consequences and more dilution than we currently anticipate with respect to our Class A common stock. We can provide no assurance as to the financial stability or viability of the option counterparties. General Risk Factors If we fail to maintain an effective system of disclosure controls and internal control over financial reporting, our ability to produce timely and accurate financial statements or comply with applicable regulations could be impaired. We are subject to the reporting requirements of the Securities Exchange Act of 1934, as amended (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 New York Stock Exchange (the NYSE). We expect that the requirements of these rules and regulations will continue to increase our legal, accounting, and financial compliance costs, make some activities more difficult, time- consuming, and costly, and place significant strain on our personnel, systems, and resources. The Sarbanes- Oxley Act requires, among other things, that we maintain effective disclosure controls and procedures and internal control over financial reporting. We are continuing to develop and refine our disclosure controls and other procedures that are designed to ensure that information required to be disclosed by us in the reports that we file with the SEC (including, without limitation, the new SEC requirement to file current reports regarding material cybersecurity incidents) 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, including accounting- related costs, and significant management oversight. In addition, our independent registered public accounting firm is required to audit the effectiveness of our internal control over financial reporting pursuant to Section 404 (b) of the Sarbanes- Oxley Act annually. Testing, or the subsequent testing by our independent registered public accounting firm, may reveal material weaknesses or significant deficiencies. If material weaknesses are identified or we are not able to comply with the requirements of Section 404 in a timely manner, our reported financial results could be materially misstated, we could receive an adverse opinion regarding our internal control over financial reporting from our independent registered public

accounting firm, we could be subject to investigations or sanctions by regulatory authorities, and we could incur substantial expenses. Our current controls and any new controls that we develop may become inadequate because of changes in conditions in our business. 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 results of operations or cause us to fail to meet our reporting obligations and may result in a restatement of our 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. 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 NYSE. Our business is subject to the risks of catastrophic events. The occurrence of any catastrophic event, including an earthquake, volcanic event, fire, flood, tsunami, the effects of climate change, or other weather event, power loss, telecommunications failure, software or hardware malfunction, epidemic or pandemic disease ~~(such as the COVID- 19 pandemic)~~, cyber attack, military conflict or war, or terrorist attack, could result in lengthy interruptions in our service. Our corporate headquarters is located in the San Francisco Bay Area and one of our core co- location facilities is located in the greater Portland, Oregon area, both regions known for seismic and / or volcanic activity, and we also have a second core co- location facility in ~~Luxembourg~~ **Amsterdam**. Our insurance coverage may not compensate us in full or at all for losses that may occur in the event of any of these potential future catastrophic events. In addition, any of these catastrophic events could cause disruptions to the Internet or the economy as a whole. Even with our disaster recovery arrangements, our service could be interrupted. 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 customers would be impaired or we could lose critical data. Our partners, suppliers, and customers are also subject to the risk of catastrophic events. In those events, our ability to deliver our products in a timely manner, as well as the demand for our products, may be divided on account of factors outside our control. Further, the effects of climate change on the global economy and the technology industry are rapidly evolving. While we seek to mitigate our business risks associated with climate change by establishing robust environmental programs and partnering with organizations who are focused on mitigating their own climate- related risks, there are inherent climate- related risks wherever business is conducted. Any of our locations may be vulnerable to the adverse effects of climate change. For example, our corporate headquarters in the San Francisco Bay Area and one of our core co- location facilities located in the greater Portland, Oregon area have experienced and may continue to experience, climate- related events and at an increasing frequency, including severe storms, floods, drought, water scarcity, heat waves, wildfires and resultant air quality impacts and power shutoffs associated with these types of events. Additionally, it will remain difficult to mitigate the impact of these events on our employees who continue to work remotely. Changing market dynamics, global policy developments and increasing frequency and impact of extreme weather events on critical infrastructure in the United States and elsewhere have the potential to disrupt our business, the business of our partners, suppliers and customers, and may cause us to experience higher attrition, losses and additional costs to maintain or resume operations. The requirements of being a public company may strain our resources, divert management' s attention, and affect our ability to attract and retain executive management and qualified board members. We are subject to the reporting requirements of the Exchange Act, the Sarbanes- Oxley Act, the Dodd- Frank Wall Street Reform and Consumer Protection Act of 2010, the listing requirements of the NYSE, and other applicable securities rules and regulations. Compliance with these rules and regulations increases our legal and financial compliance costs, makes some activities more difficult, time- consuming, or costly, and increases demand on our systems and resources. The Exchange Act requires, among other things, that we file annual, quarterly, and current reports with respect to our business and results of operations. The Sarbanes- Oxley Act requires, among other things, that we maintain effective disclosure controls and procedures and internal control over financial reporting. In order to maintain and, if required, improve our disclosure controls and procedures and internal control over financial reporting to meet this standard, significant resources and management oversight is required. We are required to disclose changes made in our internal control and procedures on a quarterly basis and to furnish a report by management on, among other things, the effectiveness of our internal control over financial reporting. In addition, our independent registered public accounting firm is required to attest to the effectiveness of our internal control over financial reporting. As a result of the complexity involved in complying with the rules and regulations applicable to public companies, our management' s attention may be diverted from other business concerns, which could adversely affect our business and results of operations. Although we have already hired additional employees and have engaged outside consultants to assist us in complying with these requirements, we may need to hire more employees in the future or engage additional outside consultants, which will increase our operating expenses. In addition, changing laws, regulations, and standards relating to corporate governance and public disclosure are creating uncertainty for public companies, increasing legal and financial compliance costs, and making some activities more time consuming. These laws, regulations, and standards are subject to varying interpretations, in many cases due to their lack of specificity, and, as a result, their application in practice may evolve over time as new guidance is provided by regulatory and governing bodies. This could result in continuing uncertainty regarding compliance matters and higher costs necessitated by ongoing revisions to disclosure and governance practices. We intend to invest substantial resources to comply with evolving laws, regulations, and standards, and this investment may result in increased general and administrative expenses and a diversion of management' s time and attention from revenue-generating activities to compliance activities. If our efforts to comply with new laws, regulations, and standards differ from the activities intended by regulatory or governing bodies due to ambiguities related to their application and practice, regulatory authorities may initiate legal proceedings against us and our business may be adversely affected. Failure to comply with the

aforementioned rules and regulations may make it more expensive for us to maintain director and officer liability insurance, and in the future we may be required to accept reduced coverage or incur substantially higher costs to obtain coverage. These factors could also make it more difficult for us to attract and retain qualified members of our Board of Directors, particularly to serve on our audit committee and compensation committee, and qualified executive officers. As a result of disclosure of information in our filings with the SEC, our business and financial condition are visible, which we believe may result in threatened or actual litigation, including by competitors and other third parties. If such claims are successful, our business and results of operations could be adversely affected, and even if the claims do not result in litigation or are resolved in our favor, these claims, and the time and resources necessary to resolve them, could divert the resources of our management and adversely affect our business and results of operations.