Risk Factors Comparison 2024-03-07 to 2023-03-09 Form: 10-K

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

A description of the risks and uncertainties associated with our business is set forth below. You should carefully consider the risks and uncertainties described below, as well as the other information in this Annual Report on Form 10- K, including our consolidated financial statements and the related notes and " Management' s Discussion and Analysis of Financial Condition and Results of Operations. " The occurrence of any of the events or developments described below, or of additional risks and uncertainties not presently known to us or that we currently deem immaterial, could materially and adversely affect our business, results of operations, financial condition and growth prospects. In such an event, the market price of our Class A common stock could decline, and you could lose all or part of your investment. Summary of Risk Factors Our business is subject to numerous risks and uncertainties, any one of which could materially adversely affect our business, results of operations, financial condition **,** and growth prospects. Below is a summary of some of these risks. This summary is not complete, and should be read together with the entire section titled " Risk Factors " in this Annual Report on Form 10- K, as well as the other information in this Annual Report on Form 10- K and the other filings that we make with the SEC. • We have experienced rapid growth in recent periods, and if we do not manage our future growth, our business and results of operations will be adversely affected. • We have a history of losses **,** and **while we have achieved profitability in quarterly periods, we** may not be able to achieve or sustain profitability in the future. • If organizations do not adopt cloud- based SaaS- delivered endpoint security solutions, our ability to grow our business and results of operations may be adversely affected. • If we are unable to successfully enhance our existing products and services and introduce new products and services in response to rapid technological changes and market developments as well as evolving security threats, our competitive position and prospects will be harmed. • If we are unable to attract new customers, our future results of operations could be harmed. • If our customers do not renew their subscriptions for our products and add additional cloud modules to their subscriptions, our future results of operations could be harmed. • Our sales cycles can be long and unpredictable, and our sales efforts require considerable time and expense, • We face intense competition and could lose market share to our competitors, which could adversely affect our business, financial condition, and results of operations. • If our solutions fail or are perceived to fail to detect or prevent incidents or have or are perceived to have defects, errors, or vulnerabilities, our brand and reputation would be harmed, which would adversely affect our business and results of operations. • As a cybersecurity provider, we have been, and expect to continue to be, a target of cyberattacks. If our internal networks, systems, or data are or are perceived to have been breached, our reputation may be damaged and our financial results may be negatively affected. • We rely on third- party data centers, such as Amazon Web Services, and our own colocation data centers, to host and operate our Falcon platform, and any disruption of or interference with our use of these facilities may negatively affect our ability to maintain the performance and reliability of our Falcon platform, which could cause our business to suffer. • We rely on our key technical, sales and management personnel to grow our business, and the loss of one or more key employees could harm our business. • If we are unable to attract and retain qualified personnel, our business could be harmed. • Our results of operations may fluctuate significantly, which could make our future results difficult to predict and could cause our results of operations to fall below expectations. • Claims by others that we infringe their proprietary technology or other intellectual property rights could result in significant costs and substantially harm our business, financial condition, results of operations, and prospects. • If we are not able to comply with applicable data protection, security, privacy, and other government- and industry- specific laws, regulations, standards or requirements, our business, results of operations, and financial condition could be harmed. • 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 and financial condition. Risks Related to Our Business and Industry We have experienced rapid revenue growth in recent periods and we expect to continue to invest broadly across our organization to support our growth. For example, our headcount grew from ~~3~~ **4** , ~~394~~ **965** employees as of January 31, ~~2021~~ **2022** , to 7, ~~273~~ **925** employees as of January 31, ~~2023~~ **2024** . Although we have experienced rapid growth historically, we may not sustain our current growth rates and our investments to support our growth may not be successful. The growth and expansion of our business will require us to invest significant financial and operational resources and the continuous dedication of our management team. Our future success will depend in part on our ability to manage our growth effectively, which will require us to, among other things: • effectively attract, integrate, and retain a large number of new employees, particularly members of our sales and marketing and research and development teams; • further improve our Falcon platform, including our cloud modules, and IT infrastructure, including expanding and optimizing our data centers, to support our business needs; • enhance 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 and customers; and • improve our financial, management, and compliance systems and controls. If we fail to achieve these objectives effectively, our ability to manage our expected growth, ensure uninterrupted operation of our Falcon platform and key business systems, and comply with the rules and regulations applicable to our business could be impaired. Additionally, the quality of our platform and services could suffer and we may not be able to adequately address competitive challenges. Any of the foregoing could adversely affect our business, results of operations, and financial condition. We have incurred net losses ~~in all periods since our inception~~ **each year prior to fiscal 2024** , and we may not achieve or maintain profitability in the future. We experienced net **gains of $ 89. 3 million for fiscal 2024, and net** losses of $ 183. 2 million, **and** $ 234. 8 ~~million, and $ 92. 6~~ million for fiscal 2023, **and** fiscal 2022, ~~and fiscal 2021,~~ respectively. As of January 31, ~~2023~~ **2024** , we had an accumulated deficit of $ 1. 1

billion. While we have experienced significant growth in revenue in recent periods, **and have achieved profitability during quarterly periods,** we cannot assure you when or whether we will reach **sustained** ~~or maintain~~ profitability. We also expect our operating expenses to increase in the future as we continue to invest for our future growth, which will negatively affect our results of operations if our total revenue does not increase. We cannot assure you that these investments will result in substantial increases in our total revenue or improvements in our results of operations. We also have incurred and expect to continue to incur significant additional legal, accounting, and other expenses as a public company. Any failure to increase our revenue as we invest in our business or to manage our costs could prevent us from achieving or maintaining profitability or positive cash flow. We believe our future success will depend in large part on the growth, if any, in the market for cloud- based SaaS- delivered endpoint security solutions. The use of SaaS solutions to manage and automate security and IT operations is at an early stage and rapidly evolving. As such, it is difficult to predict its potential growth, if any, customer adoption and retention rates, customer demand for our solutions, customer consolidation on our platform, or the success of existing competitive products. Any expansion in our market depends on a number of factors, including the cost, performance, and perceived value associated with our solutions and those of our competitors. If our solutions do not achieve widespread adoption or there is a reduction in demand for our solutions due to a lack of customer acceptance, technological challenges, competing products, privacy concerns, decreases in corporate spending, weakening economic conditions or otherwise, it could result in early terminations, reduced customer retention rates, or decreased revenue, any of which would adversely affect our business, results of operations, and financial results. We do not know whether the trend in adoption of cloud- based SaaS- delivered endpoint security solutions we have experienced in the past will continue in the future. Furthermore, if we or other SaaS security providers experience security incidents, loss or disclosure of customer data, disruptions in delivery, or other problems, the market for SaaS solutions as a whole, including our security solutions, could be negatively affected. You should consider our business and prospects in light of the risks and difficulties we encounter in this new and evolving market. Our ability to increase revenue from existing customers and attract new customers will depend in significant part on our ability to anticipate and respond effectively to rapid technological changes and market developments as well as evolving security threats. The success of our Falcon platform depends on our ability to take such changes into account and invest effectively in our research and development organization to increase the reliability, availability and scalability of our existing solutions and introduce new solutions. If we fail to effectively anticipate, identify or respond to such changes in a timely manner, or at all, our business could be harmed. Even if we adequately fund our research and development efforts there is no guarantee that we will realize a return on such efforts. Success in delivering enhancements and new solutions depends on several factors, including the timely completion, introduction and market acceptance of the enhancement or new solution, the risk that such enhancement or new solution may have quality or other defects or deficiencies, especially in the early stages of introduction, as well as our ability to seamlessly integrate all of our product and service offerings and develop adequate sales capabilities in new markets. Failure ~~in this regard~~ **to effectively deliver, integrate, and manage perceptions with respect to enhancements and new solutions** may erode our competitive position, significantly impair our revenue growth, and negatively impact our operating results. To expand our customer base, we need to convince potential customers to allocate a portion of their discretionary budgets to purchase our Falcon platform. Our sales efforts often involve educating our prospective customers about the uses and benefits of our Falcon platform. Enterprises and governments that use legacy security products, such as signature- based or malware- based products, firewalls, intrusion prevention systems, and antivirus, for their IT security may be hesitant to purchase our Falcon platform if they believe that these products are more cost effective, provide substantially the same functionality as our Falcon platform or provide a level of IT security that is sufficient to meet their needs. We may have difficulty convincing prospective customers of the value of adopting our solution. Even if we are successful in convincing prospective customers that a cloud native platform like ours is critical to protect against cyberattacks, they may not decide to purchase our Falcon platform for a variety of reasons, some of which are out of our control. For example, any deterioration in general economic conditions, including as a result of the geopolitical environment, the outbreak of diseases ~~such as COVID- 19~~ **or other public health crises, volatility in the banking and financial services sector,** or inflation (as well as government policies such as raising interest rates in response to inflation), have in the past and may in the future cause our current and prospective customers to delay or cut their overall security and IT operations spending, and such delays or cuts may fall disproportionately on cloud- based security solutions like ours. Economic weakness, customer financial difficulties, and constrained spending on security and IT operations may result in decreased revenue, reduced sales, an increase in multi- phase subscription start dates, shorter terms for customer subscriptions, lengthened sales cycles, increased churn, lower demand for our products, and adversely affect our results of operations and financial conditions. Furthermore, we may need to exercise more flexibility in customer payment terms as customers navigate a more challenging economic environment. Additionally, if the incidence of cyberattacks were to decline, or be perceived to decline, or if organizations adopt endpoints that use operating systems we do not adequately support, our ability to attract new customers and expand sales of our solutions to existing customers could be adversely affected. If organizations do not continue to adopt our Falcon platform, our sales will not grow as quickly as anticipated, or at all, and our business, results of operations, and financial condition would be harmed. In order for us to maintain or improve our results of operations, it is important that our customers renew their subscriptions for our Falcon platform when existing contract terms expire, and that we expand our commercial relationships with our existing customers by selling additional cloud modules and by deploying to more endpoints in their environments. Our customers have no obligation to renew their subscription for our Falcon platform after the expiration of their contractual subscription period, which is generally one year, and in the normal course of business, some customers have elected not to renew. In addition, customers that previously signed multi- year subscription contracts may renew for shorter contract subscription lengths, and customers may cease using certain cloud modules altogether. Even if customers choose to renew their subscription of certain cloud modules, they may decline to purchase additional cloud modules or choose not to consolidate onto our Falcon platform. Our customer retention and expansion may decline or fluctuate as a result of a number of factors, including

our customers' satisfaction with our services, our pricing, customer security and networking issues and requirements, our customers' spending levels, decreases in the number of endpoints to which our customers deploy our solutions, mergers and acquisitions involving our customers, industry developments, competition and general economic and geopolitical conditions. If our efforts to maintain and expand our relationships with our existing customers are not successful, our business, results of operations, and financial condition may materially suffer. Our sales cycles can be long and unpredictable, and our sales efforts require considerable time and expense. Our revenue recognition is difficult to predict because of the length and unpredictability of the sales cycle for our Falcon platform. Customers often view the subscription to our Falcon platform as a significant strategic decision and, as a result, frequently require considerable time to evaluate, test and qualify our Falcon platform prior to entering into or expanding a relationship with us. Large enterprises and government entities in particular often undertake a significant evaluation process that further lengthens and adds uncertainty to our sales cycle. In addition, uncertain economic conditions may lead to additional scrutiny of budgets by current and prospective customers, which has resulted in, for example, longer sales cycles for products and services, and may result in shifting demand for IT products and services, and slower adoption of new technologies. Our direct sales team develops relationships with our customers, and works with our channel partners on account penetration, account coordination, sales and overall market development. We spend substantial time and resources on our sales efforts without any assurance that our efforts will produce a sale. Security solution purchases are frequently subject to budget constraints, multiple approvals and unanticipated administrative, processing and other delays. As a result, it is difficult to predict whether and when a sale will be completed. The failure of our efforts to secure sales after investing resources in a lengthy sales process could adversely affect our business and results of operations. The market for security and IT operations solutions is intensely competitive, fragmented, and characterized by rapid changes in technology, customer requirements, industry standards, increasingly sophisticated attackers, and by frequent introductions of new or improved products **or services** to combat security threats. We expect to continue to face intense competition from current competitors, as well as from new entrants into the market. If we are unable to anticipate or react to these challenges, our competitive position could weaken, and we could experience a decline in revenue or reduced revenue growth, and loss of market share that would adversely affect our business, financial condition, and results of operations. Our ability to compete effectively depends upon numerous factors, many of which are beyond our control, including, but not limited to: • product capabilities, including performance and reliability, of our Falcon platform, including our cloud modules, services, and features compared to those of our competitors; • our ability, and the ability of our competitors, to improve existing products, services, and features, or to develop new ones to address evolving customer needs; • our ability to attract, retain, and motivate talented employees; • our ability to establish and maintain relationships with channel partners; • the strength of our sales and marketing efforts; and • acquisitions or consolidation within our industry, which may result in more formidable competitors. Our competitors include the following by general category: • legacy antivirus product providers who offer a broad range of approaches and solutions including traditional signature- based anti- virus protection; • alternative endpoint security providers who generally offer a mix of on- premise and cloud- hosted products that rely heavily on malware- only or application whitelisting techniques; • network security vendors who are supplementing their core perimeter- based offerings with endpoint **or cloud** security solutions **; • cloud security vendors, including those who focus on public cloud infrastructure and services; • identify security vendors that seek to identify and secure user accounts and related activities** ; and • professional service providers who offer cybersecurity response services. Many of our competitors have greater financial, technical, marketing, sales, and other resources, greater name recognition, longer operating histories, and a larger base of customers than we do. They may be able to devote greater resources to the development, promotion, and sale of services than we can, and they may offer lower pricing than we do. Further, they may have greater resources for research and development of new technologies, the provision of customer support, and the pursuit of acquisitions. Our larger competitors have substantially broader and more diverse product and services offerings as well as routes to market, which allows them to leverage their relationships based on other products or incorporate functionality into existing products to gain business in a manner that discourages users from purchasing our platform, including our cloud modules. Conditions in our market could change rapidly and significantly as a result of technological advancements, **including with respect to AI. Our competitors may more successfully incorporate AI into their products, gain or leverage superior access to certain AI technologies, and achieve higher market acceptance of their AI solutions. Conditions in our market could also change rapidly and significantly due to** partnering or acquisitions by our competitors or continuing market consolidation. Some of our competitors have recently made acquisitions of businesses or have established cooperative relationships that may allow them to offer more directly competitive and comprehensive solutions than were previously offered and adapt more quickly to new technologies and customer needs. These competitive pressures in our market or our failure to compete effectively may result in price reductions, fewer orders, reduced revenue and gross margins, increased net losses and loss of market share. Further, competitors that specialize in providing protection from a single type of security threat may be able to deliver these targeted security products to the market quicker than we can or convince organizations that these limited products meet their needs. Even if there is significant demand for cloud- based security solutions like ours, if our competitors include functionality that is, or is perceived to be, equivalent to or better than ours in legacy products that are already generally accepted as necessary components of an organization' s IT security architecture, we may have difficulty increasing the market penetration of our platform. Furthermore, even if the functionality offered by other security and IT operations providers is more limited than the functionality of our platform, organizations may elect to accept such limited functionality in lieu of adding products from additional vendors like us. If we are unable to compete successfully, or if competing successfully requires us to take aggressive pricing or other actions, our business, financial condition, and results of operations would be adversely affected. Competitive pricing pressure may reduce our gross profits and adversely affect our financial results. If we are unable to maintain our pricing due to competitive pressures or other factors, our margins will be reduced and our gross profits, business, results of operations, and financial condition would be adversely affected. The subscription prices for our Falcon platform, cloud modules, and

professional services may decline for a variety of reasons, including competitive pricing pressures, discounts, anticipation of the introduction of new solutions by our competitors, or promotional programs offered by us or our competitors. The cybersecurity market remains very competitive, and competition may further increase in the future. Competitors may reduce the price of products or subscriptions that compete with ours or may bundle them with other products and subscriptions. Real or perceived defects, errors or vulnerabilities in our Falcon platform and cloud modules, the failure of our platform to detect or prevent incidents, including advanced and newly developed attacks, misconfiguration of our solutions, or the failure of customers to take action on attacks identified by our platform could harm our reputation and adversely affect our business, financial position and results of operations. Because our cloud native security platform is complex, it may contain defects or errors that are not detected until after deployment. We cannot assure you that our products will detect all cyberattacks, especially in light of the rapidly changing security threat landscape that our solution seeks to address. Due to a variety of both internal and external factors, including, without limitation, defects or misconfigurations of our **or third- party** solutions, our solutions could be or become vulnerable to security incidents (both from intentional attacks and accidental causes) that cause them to fail to secure endpoints and detect and block attacks. In addition, because the techniques used by computer hackers to access or sabotage networks and endpoints change frequently and generally are not recognized until launched against a target, there is a risk that an advanced attack could emerge that our cloud native security platform is unable to detect or prevent until after some of our customers are affected. Additionally, our Falcon platform may falsely indicate a cyberattack or threat that does not actually exist, which may lessen customers' trust in our solutions. Moreover, as our cloud native security platform is adopted by an increasing number of enterprises and governments, individuals and organizations behind advanced cyberattacks may intensify their efforts to defeat our security platform. If this happens, our systems and subscription customers could be specifically targeted by attackers and could result in vulnerabilities in our platform or undermine the market acceptance of our Falcon platform and could adversely affect our reputation as a provider of security solutions. Because we host customer data on our cloud platform, which in some cases may contain personally- identifiable information or potentially confidential information, a security compromise, or an accidental or intentional misconfiguration or malfunction of our platform **or third- party platforms** could result in personally- identifiable information and other customer data being accessible such as to attackers or to other customers. Further, if a high profile security breach occurs with respect to another next- generation or cloud- based security system, our customers and potential customers may lose trust in cloud solutions generally, and cloud- based security solutions such as ours in particular. Organizations are increasingly subject to a wide variety of attacks on their networks, systems, and endpoints. No security solution, including our Falcon platform, can address all possible security threats or block all methods of penetrating a network or otherwise perpetrating a security incident. If any of our customers experiences a successful cyberattack while using our solutions or services, such customer could be disappointed with our Falcon platform, regardless of whether our solutions or services blocked the theft of any of such customer' s data **, if the customer failed to protect its own credentials** , or if the attack would have otherwise been mitigated or prevented if the customer had fully deployed aspects of our Falcon platform. Similarly, if our solutions detect attacks against a customer but the customer does not address the vulnerability, customers and the public may erroneously believe that our solutions were not effective. Security breaches against customers that use our solutions may result in customers and the public believing that our solutions failed. Our Falcon platform may fail to detect or prevent malware, viruses, worms or similar threats for any number of reasons, including our failure to enhance and expand our Falcon platform to reflect the increasing sophistication of malware, viruses and other threats. Real or perceived security breaches of our customers' networks could cause disruption or damage to their networks or other negative consequences and could result in negative publicity to us, damage to our reputation, and other customer relations issues, and may adversely affect our revenue and results of operations. As a cybersecurity provider, we have been, and expect to continue to be, a target of cyberattacks. If our or our service providers' internal networks, systems, or data are or are perceived to have been compromised, our reputation may be damaged and our financial results may be negatively affected. As a provider of security solutions, we have in the past been, and may in the future be, specifically targeted by bad actors for attacks intended to circumvent our security capabilities or to exploit our Falcon platform as an entry point into customers' endpoints, networks, or systems. In particular, because we have been involved in the identification of organized cybercriminals and nation- state actors, we have been the subject of intense efforts by sophisticated cyber adversaries who seek to compromise our systems. Such efforts may also intensify ~~if~~ **as** geopolitical tensions increase. We are also susceptible to inadvertent compromises of our systems and data, including those arising from process, coding, or human errors. ~~We also~~ **Moreover, we** utilize third- party service providers to, among other things, host, transmit, or otherwise process electronic data in connection with our business activities, including our supply chain, operations, and communications. Our third- party service providers and other vendors have faced and may continue to face cyberattacks, compromises, interruptions in service, or other security incidents from a variety of sources. A successful attack or other incident that results in an interruption of service or that compromises our or our service providers' internal networks, systems, or data could have a significant negative effect on our operations, reputation, financial resources, and the value of our intellectual property. We cannot assure you that any of our efforts to manage this risk, including adoption of a comprehensive incident response plan and process for detecting, mitigating, and investigating security incidents that we regularly test through table- top exercises, testing of our security protocols through additional techniques, such as penetration testing, debriefing after security incidents, to improve our security and responses, and regular briefing of our directors and officers on our cybersecurity risks, preparedness, and management, will be effective in protecting us from such attacks. It is virtually impossible for us to entirely eliminate the risk of such attacks, compromises, interruptions in service, or other security incidents affecting our internal systems or data, or that of our third- party service providers and vendors. Organizations are subject to a wide variety of attacks on their supply chain, networks, systems, and endpoints, and techniques used to sabotage or to obtain unauthorized access to networks in which data is stored or through which data is transmitted change frequently. Furthermore, employee error or malicious activity could compromise our systems. As a result, we may be unable to anticipate

these techniques or implement adequate measures to prevent an intrusion into our networks, which could result in unauthorized access to customer data, intellectual property including access to our source code, and information about vulnerabilities in our product, which in turn, could reduce the effectiveness of our solutions, or lead to cyberattacks or other intrusions of our customers' networks, litigation, governmental audits and investigations and significant legal fees, any or all of which could damage our relationships with our existing customers and could have a negative effect on our ability to attract and retain new customers. We have expended, and anticipate continuing to expend, significant resources in an effort to prevent security breaches and other security incidents impacting our systems and data. Since our business is focused on providing reliable security services to our customers, we believe that an actual or perceived security incident affecting our internal systems or data or data of our customers would be especially detrimental to our reputation, customer confidence in our solution, and our business. In addition, while we maintain insurance policies that may cover certain liabilities in connection with a cybersecurity incident, we cannot be certain that our insurance coverage will be adequate for liabilities actually incurred, that insurance will continue to be available to us on commercially 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, including our financial condition, results of operations and reputation. We rely on third- party data centers, such as Amazon Web Services, and our own colocation data centers to host and operate our Falcon platform, and any disruption of or interference with our use of these facilities may negatively affect our ability to maintain the performance and reliability of our Falcon platform which could cause our business to suffer. Our customers depend on the continuous availability of our Falcon platform. We currently host our Falcon platform and serve our customers using a mix of third- party data centers, primarily Amazon Web Services, Inc., or AWS, and our data centers, hosted in colocation 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. We have experienced, and expect that in the future we may experience interruptions, delays and outages in service and availability from time to time due to a variety of factors, including infrastructure changes, human or software errors, website hosting disruptions and capacity constraints. The following factors, many of which are beyond our control, can affect the delivery, availability, and the performance of our Falcon platform: • the development and maintenance of the infrastructure of the internet; • the performance and availability of third- party providers of cloud infrastructure services, such as AWS, with the necessary speed, data capacity and security for providing reliable internet access and services; • decisions by the owners and operators of the data centers where our cloud infrastructure is deployed to terminate our contracts, discontinue services to us, shut down operations or facilities, increase prices, change service levels, limit bandwidth, declare bankruptcy or prioritize the traffic of other parties; • physical or electronic break- ins, acts of war or terrorism, human error or interference (including by disgruntled employees, former employees or contractors) and other catastrophic events; • cyberattacks, including denial of service attacks, targeted at us, our data centers, or the infrastructure of the internet; • failure by us to maintain and update our cloud infrastructure to meet our data capacity requirements; • errors, defects or performance problems in our software, including third- party software incorporated in our software; • improper deployment or configuration of our solutions; • the failure of our redundancy systems, in the event of a service disruption at one of our data centers, to provide failover to other data centers in our data center network; and • the failure of our disaster recovery and business continuity arrangements. The adverse effects of any service interruptions on our reputation, results of operations, and financial condition may be disproportionately heightened due to the nature of our business and the fact that our customers have a low tolerance for interruptions of any duration. Interruptions or failures in our service delivery could result in a cyberattack or other security threat to one of our customers during such periods of interruption or failure. Additionally, interruptions or failures in our service could cause customers to terminate their subscriptions with us, adversely affect our renewal rates, and harm our ability to attract new customers. Our business would also be harmed if our customers believe that a cloud- based SaaS- delivered endpoint security solution is unreliable. While we do not consider them to have been material, we have experienced, and may in the future experience, service interruptions and other performance problems due to a variety of factors. The occurrence of any of these factors, or if we are unable to rapidly and cost- effectively fix such errors or other problems that may be identified, could damage our reputation, negatively affect our relationship with our customers or otherwise harm our business, results of operations and financial condition. Our future success is substantially dependent on our ability to attract, 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 George Kurtz, our President and Chief Executive Officer, who is critical to our future vision and strategic direction. We rely on our leadership team in the areas of operations, security, research and development, marketing, sales, support and general and administrative functions. Although we have entered into employment agreements with our key personnel, our employees, including our executive officers, work for us on an " at- will " basis, which means they may terminate their employment with us at any time. Leadership transitions can be inherently difficult to manage. In particular, they can cause operational and administrative inefficiencies, and could impact relationships with key customers and vendors. If Mr. Kurtz, or one or more of our key employees, or members of our management team resigns or otherwise ceases to provide us with their service, our business could be harmed. There is also significant competition for personnel with the skills and technical knowledge that we require across our technology, cyber, sales, professional services, and administrative support functions. Competition for these personnel is intense, especially for experienced sales professionals and for engineers experienced in designing and developing cloud applications and security software. We have from time to time experienced, and we expect to continue to experience, difficulty in hiring and retaining employees with appropriate qualifications. For example, in recent years, recruiting, hiring and retaining employees with expertise in the cybersecurity industry has become increasingly difficult as the demand for cybersecurity professionals has increased as a result of the recent cybersecurity attacks on global corporations and governments. Additionally, our incident response and proactive services team is small and comprised of personnel with highly

technical skills and experience, who are in high demand, and who would be difficult to replace. More generally, the technology industry is subject to substantial and continuous competition for engineers with high levels of experience in designing, developing and managing software and Internet- related services. Many of the companies with which we compete for experienced personnel have greater resources than we have. Our competitors also may be successful in recruiting and hiring members of our management team or other key employees, and it may be difficult for us to find suitable replacements on a timely basis, on competitive terms, or at all. We have in the past, and may in the future, be subject to allegations that employees we hire have been improperly solicited, or that they have divulged proprietary or other confidential information or that their former employers own such employees' inventions or other work product, or that they have been hired in violation of non-compete provisions or non- solicitation provisions. In addition, job candidates and existing employees often consider the value of the equity awards they receive in connection with their employment. Volatility or lack of performance in our stock price may also affect our ability to attract and retain our key employees. Also, many of our employees have become, or will soon become, vested in a substantial amount of equity awards, which may give them 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 adversely affect our business, results of operations and financial condition. If we do not effectively expand and train our direct sales force, we may be unable to add new customers or increase sales to our existing customers, and our business will be adversely affected. We depend on our direct sales force to obtain new customers and increase sales with existing customers. Our ability to achieve significant revenue growth will depend, in large part, on our success in recruiting, training and retaining sufficient numbers of sales personnel, particularly in international markets. We have expanded our sales organization significantly in recent periods and expect to continue to add additional sales capabilities in the near term. There is significant competition for sales personnel with the skills and technical knowledge that we require. New hires require significant training and may take significant time before they achieve full productivity, and this delay is accentuated by our long sales cycles. Our recent hires and planned hires may not become productive as quickly as we expect, and we may be unable to hire or retain sufficient numbers of qualified individuals in the markets where we do business or plan to do business. In addition, a large percentage of our sales force is new to our company and selling our solutions, and therefore this team may be less effective than our more seasoned sales personnel. Furthermore, hiring sales personnel in new countries, or expanding our existing presence, requires upfront and ongoing expenditures that we may not recover if the sales personnel fail to achieve full productivity. We cannot predict whether, 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 and train 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 results of operations will be adversely affected. Because we recognize revenue from subscriptions to our platform over the term of the subscription, downturns or upturns in new business will not be immediately reflected in our results of operations. We generally recognize revenue from customers ratably over the terms of their subscription, which is generally one year. As a result, a substantial portion of the revenue we report in each period is attributable to the recognition of deferred revenue relating to agreements that we entered into during previous periods. Consequently, any increase or decline in new sales or renewals in any one period will not be immediately reflected in our revenue for that period. Any such change, however, would affect our revenue in future periods. Accordingly, the effect of downturns or upturns in new sales and potential changes in our rate of renewals may not be fully reflected in our results of operations until future periods. We may also be unable to timely reduce our cost structure in line with a significant deterioration in sales or renewals that would adversely affect our results of operations and financial condition. Our results of operations may vary significantly from period to period, which could adversely affect our business, financial condition and results of operations. Our results of operations have varied significantly from period to period, and we expect that our results of operations will continue to vary as a result of a number of factors, many of which are outside of our control and may be difficult to predict, including: • our ability to attract new and retain existing customers; • the budgeting cycles, seasonal buying patterns, and purchasing practices of customers; • economic difficulties confronting our customers, which may impact the number of modules or endpoint deployments they are willing or able to purchase; • **insolvency or credit difficulties confronting our customers, affecting their ability to purchase or pay for our solutions; •** the timing and length of our sales cycles; • changes in customer or channel partner requirements or market needs **; • any disruption in our relationship with channel partners** ; • changes in the growth rate of the cloud- based SaaS- delivered endpoint security solutions market; • the timing and success of new product and service introductions by us or our competitors or any other competitive developments, including consolidation among our customers or competitors; • ~~the level of awareness of cybersecurity threats, particularly advanced cyberattacks, and the market adoption of our Falcon platform; • our ability to successfully expand our business domestically and internationally; •~~ decisions by organizations to purchase security solutions from larger, more established security vendors or from their primary IT equipment vendors; • changes in our pricing policies or those of our competitors; • ~~any disruption in our relationship with channel partners; • insolvency~~ **the level of awareness of cybersecurity threats, particularly advanced cyberattacks, and the market adoption of** ~~or~~ **our Falcon platform** ~~credit difficulties confronting our customers, affecting their ability to purchase or pay for our solutions~~ ; • significant security breaches of, technical difficulties with or interruptions to, the use of our Falcon platform **; • negative media coverage or publicity; • our ability to successfully expand our business domestically and internationally; • the amount and timing of operating costs (including new hires), tightening of labor markets and capital expenditures related to the expansion of our business** ; • extraordinary expenses such as litigation or other dispute- related settlement payments or outcomes; • ~~future accounting pronouncements or changes in our accounting policies or practices; • negative media coverage or publicity; • political events; • the amount and timing of operating costs and capital expenditures related to the expansion of our business; •~~ increases or decreases in our expenses caused by fluctuations in foreign currency exchange rates; ~~and~~ • **future accounting pronouncements**

~~significant natural disasters and other catastrophic events, including the occurrence of a contagious disease or illness, such as COVID- 19. Furthermore, our~~ **or** ~~business and revenues are impacted by~~ **changes in our accounting policies or practices; • deteriorating or volatile conditions in the** global ~~economic~~ **economy** and ~~geopolitical conditions. Volatile~~ financial markets, ~~inflation~~ **including as a result of weak or negative gross domestic product growth** , ~~rising~~ **uncertainty or disruptions in the capital and credit markets, changing** interest rates, **inflation, bank failures or adverse conditions impacting financial institutions, and** supply ~~-~~ chain ~~challenges,~~ **disruptions; and •** political **events** ~~turmoil and other disruptions to global and regional economies and markets continue to add uncertainty to macroeconomic conditions. Any continued or further uncertainty~~ , ~~weakness or deterioration in economic conditions or the~~ geopolitical **unrest** ~~environment could harm our~~ **or** ~~business and results~~ **tension, acts** of ~~operations~~ **war and terrorism** . In addition, we experience seasonal fluctuations in our financial results as we typically receive a higher percentage of our annual orders from new customers, as well as renewal orders from existing customers, in the second half of the fiscal year as compared to the first half of the year due to the annual budget approval process of many of our customers. In addition, we also experience seasonality in our operating margin, typically with a lower margin in the first half of our fiscal year. Any of the above factors, individually or in the aggregate, may result in significant fluctuations in our financial and other results of operations from period to period. As a result of this variability, our historical results of operations should not be relied upon as an indication of future performance. Moreover, this variability and unpredictability could result in our failure to meet our operating plan or the expectations of investors or analysts for any period. If we fail to meet such expectations for these or other reasons, our stock price could fall substantially, and we could face costly lawsuits, including securities class action suits. If we are not able to maintain and enhance our CrowdStrike and Falcon brand and our reputation as a provider of high- efficacy security solutions, our business and results of operations may be adversely affected. We believe that maintaining and enhancing our CrowdStrike and Falcon brand and our reputation as a provider of high-efficacy security solutions is critical to our relationship with our existing customers, channel partners, and technology alliance partners and our ability to attract new customers and partners. The successful promotion of our CrowdStrike and Falcon brand will depend on a number of factors, including our marketing efforts, our ability to continue to develop additional cloud modules and features for our Falcon platform, our ability to successfully differentiate our Falcon platform from competitive cloud- based or legacy security solutions and, ultimately, our ability to detect and stop breaches. Although we believe it is important for our growth, our brand promotion activities may not be successful or yield increased revenue. In addition, independent industry or financial analysts and research firms often test our solutions and provide reviews of our Falcon platform, as well as the products of our competitors, and perception of our Falcon platform in the marketplace may be significantly influenced by these reviews. If these reviews are negative, or less positive as compared to those of our competitors' products, our brand may be adversely affected. Our solutions may fail to detect or prevent threats in any particular test for a number of reasons that may or may not be related to the efficacy of our solutions in real world environments. To the extent potential customers, industry analysts or testing firms believe that the occurrence of a failure to detect or prevent any particular threat is a flaw or indicates that our solutions or services do not provide significant value, we may lose customers, and our reputation, financial condition and business would be harmed. Additionally, the performance of our channel partners and technology alliance partners may affect our brand and reputation if customers do not have a positive experience with these partners. In addition, we have in the past worked, and continue to work, with high profile private and public customers as well as assist in analyzing and remediating high profile cyberattacks, which sometimes involve nation- state actors. Our work with such customers has exposed us to publicity and media coverage. Changing political environments in the United States and abroad may amplify the media and political scrutiny we face. Negative publicity about us, including about our management, the efficacy and reliability of our Falcon platform, our products offerings, our professional services, and the customers we work with, even if inaccurate, could adversely affect our reputation and brand. If we are unable to maintain successful relationships with our channel partners and technology alliance partners, or if our channel partners or technology alliance partners fail to perform, our ability to market, sell and distribute our Falcon platform will be limited, and our business, financial position and results of operations will be harmed. In addition to our direct sales force, we rely on our channel partners to sell and support our Falcon platform. The vast majority of sales of our Falcon platform flow through our channel partners, and we expect this to continue for the foreseeable future. Additionally, we have entered, and intend to continue to enter, into technology alliance partnerships with third parties to support our future growth plans. The loss of a substantial number of our channel partners or technology alliance partners, or the failure to recruit additional partners, could adversely affect our results of operations. Our ability to achieve revenue growth in the future will depend in part on our success in maintaining successful relationships with our channel partners and in training our channel partners to independently sell and deploy our Falcon platform. If we fail to effectively manage our existing sales channels, or if our channel partners are unsuccessful in fulfilling the orders for our solutions, or if we are unable to enter into arrangements with, and retain a sufficient number of, high quality channel partners in each of the regions in which we sell solutions and keep them motivated to sell our products, our ability to sell our products and results of operations will be harmed. Our international operations and plans for future international expansion expose us to significant risks, and failure to manage those risks could adversely impact our business. We derived approximately **32 %,** 30 ~~%, 28~~ %, and 28 % of our total revenue from our international customers for fiscal **2024, fiscal** 2023, **and** fiscal 2022 ~~, and fiscal 2021~~ , respectively. We are continuing to adapt to and develop strategies to address international markets and our growth strategy includes expansion into target geographies, but there is no guarantee that such efforts will be successful. We expect that our international activities will continue to grow in the future, as we continue to pursue opportunities in international markets. These international operations will require significant management attention and financial resources and are subject to substantial risks, including: • greater difficulty in negotiating contracts with standard terms, enforcing contracts and managing collections, and longer collection periods; • higher costs of doing business internationally, including costs incurred in establishing and maintaining office space and equipment for our international operations; • management communication and integration problems resulting from cultural and geographic dispersion; • risks

associated with trade restrictions and foreign legal requirements, including any importation, certification, and localization of our Falcon platform that may be required in foreign countries; • greater risk of unexpected changes in regulatory practices, tariffs, and tax laws and treaties; • compliance with anti- bribery laws, including, without limitation, compliance with the U. S. Foreign Corrupt Practices Act of 1977, as amended, or FCPA, the U. S. Travel Act and the U. K. Bribery Act 2010, or Bribery Act, violations of which could lead to significant fines, penalties, and collateral consequences for our company; • heightened risk of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales arrangements that may impact financial results and result in restatements of, or irregularities in, financial statements; • the uncertainty of protection for intellectual property rights in some countries; • general economic and political conditions in these foreign markets; • foreign exchange controls or tax regulations that might prevent us from repatriating cash earned outside the United States; • political and economic instability in some countries; • double taxation of our international earnings and potentially adverse tax consequences due to changes in the tax laws of the United States or the foreign jurisdictions in which we operate; • unexpected costs for the localization of our services, including translation into foreign languages and adaptation for local practices and regulatory requirements (including, but not limited to data localization requirements); • requirements to comply with foreign privacy, data protection, and information security laws and regulations and the risks and costs of noncompliance; • greater difficulty in identifying, attracting and retaining local qualified personnel, and the costs and expenses associated with such activities; • greater difficulty identifying qualified channel partners and maintaining successful relationships with such partners; • differing employment practices and labor relations issues; and • difficulties in managing and staffing international offices and increased travel, infrastructure, and legal compliance costs associated with multiple international locations. Additionally, nearly all of our sales contracts are currently denominated in U. S. dollars. However, a strengthening of the U. S. dollar could increase the cost of our solutions to our international customers, which could adversely affect our business and results of operations. In addition, an increasing portion of our operating expenses is incurred outside the United States; is denominated in foreign currencies, such as the Australian Dollar, British Pound, Canadian Dollar, Euro, Indian Rupee, and Japanese Yen; and is subject to fluctuations due to changes in foreign currency exchange rates. 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 adversely affected. As we continue to develop and grow our business globally, our success will depend in large part on our ability to anticipate and effectively manage these risks. 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. Our business depends, in part, on sales to government organizations, and significant changes in the contracting or fiscal policies of such government organizations could have an adverse effect on our business and results of operations. Our future growth depends, in part, on increasing sales to government organizations. Demand from government organizations is often unpredictable, subject to budgetary uncertainty and typically involves long sales cycles. We have made significant investment to address the government sector, but we cannot assure you that these investments will be successful, or that we will be able to maintain or grow our revenue from the government sector. U. S. federal, state and local government sales as well as foreign government sales are subject to a number of challenges and risks that may adversely impact our business. Sales to such government entities include, but are not limited to, the following risks: • selling to governmental agencies can be highly competitive, expensive and time consuming, often requiring significant upfront time and expense without any assurance that such efforts will generate a sale; • we may be required to obtain personnel security clearances and facility clearances to perform on classified contracts for government agencies, and there is no guarantee that we will be able to obtain or maintain such clearances; • government certification, software supply chain, or source code transparency requirements applicable to us or our products are constantly evolving and, in doing so, restrict our ability to sell to certain government customers until we have attained the new or revised certification or meet other applicable requirements, which we are not guaranteed to do. For example, although we are currently certified under the U. S. Federal Risk and Authorization Management Program, or FedRAMP, such certification is costly to maintain and if we lose our certification it would restrict our ability to sell to government customers; • government product requirements are often technically complex and assessors may require us to make costly changes to our products to meet such requirements without any assurance that such changes will generate a sale; • government demand and payment for our Falcon platform may be impacted by public sector budgetary cycles and funding authorizations, with funding reductions or delays in the government appropriations or procurement processes adversely affecting public sector demand for our Falcon platform, including as a result of abrupt events such as war, incidents of terrorism, natural disasters, and public health concerns or epidemics; • government attitudes towards us as a company, our platform or the capabilities that we offer as a viable software solution may change, and reduce interest in our products and services as acceptable solutions; • changes in the political environment, including before or after a change to the leadership within the government administration, can create uncertainty or changes in policy or priorities and reduce available funding for our products and services; • third parties may compete intensely with us on pending, new or existing contracts with government products, which can also lead to appeals, disputes, or litigation relating to government procurement, including but not limited to bid protests by unsuccessful bidders on potential or actual awards of contracts to us or our partners by the government; • even if we are awarded a sale, the terms of such contracts may be unusually burdensome; • governments routinely investigate and audit government contractors' administrative processes, and any unfavorable audit could result in the government refusing to continue buying our Falcon platform, which would adversely impact our revenue and results of operations, or institute fines or civil or criminal liability if the audit were to uncover improper or illegal activities; and • governments may require certain products to be manufactured, hosted, or accessed solely in their country or in other relatively high- cost manufacturing locations, and we may not manufacture all products in locations that meet these requirements, affecting our ability to sell these products to governmental agencies. The occurrence of any of the foregoing risks could cause governments and governmental agencies to delay or refrain from purchasing our solutions in the future or

otherwise have an adverse effect on our business and results of operations. We may not timely and cost- effectively scale and adapt our existing technology to meet our customers' performance and other requirements. Our future growth is dependent upon our ability to continue to meet the needs of new customers and the expanding needs of our existing customers as their use of our solutions grow. As our customers gain more experience with our solutions, the number of endpoints and events, the amount of data transferred, processed and stored by us, the number of locations where our platform and services are being accessed, have in the past, and may in the future, expand rapidly. In order to meet the performance and other requirements of our customers, we intend to continue to make significant investments to increase capacity and to develop and implement new technologies in our service and cloud infrastructure operations. These technologies, which include databases, applications and server optimizations, network and hosting strategies, and automation, are often advanced, complex, new and untested. We may not be successful in developing or implementing these technologies. In addition, it takes a significant amount of time to plan, develop and test improvements to our technologies and infrastructure, and we may not be able to accurately forecast demand or predict the results we will realize from such improvements. To the extent that we do not effectively scale our operations to meet the needs of our growing customer base and to maintain performance as our customers expand their use of our solutions, we may not be able to grow as quickly as we anticipate, our customers may reduce or cancel use of our solutions and we may be unable to compete as effectively and our business and results of operations may be harmed. Additionally, we have and will continue to make substantial investments to support growth at our data centers and improve the profitability of our cloud platform. For example, because of the importance of AWS' services to our business and AWS' position in the cloud- based server industry, any renegotiation or renewal of our agreement with AWS may be on terms that are significantly less favorable to us than our current agreement. If our cloud- based server costs were to increase, our business, results of operations and financial condition may be adversely affected. Although we expect that we could receive similar services from other third parties, if any of our arrangements with AWS are terminated, we could experience interruptions on our Falcon platform and in our ability to make our solutions available to customers, as well as delays and additional expenses in arranging alternative cloud infrastructure services. Ongoing improvements to cloud infrastructure may be more expensive than we anticipate, and may not yield the expected savings in operating costs or the expected performance benefits. In addition, we may be required to re- invest any cost savings achieved from prior cloud infrastructure improvements in future infrastructure projects to maintain the levels of service required by our customers. We may not be able to maintain or achieve cost savings from our investments, which could harm our financial results. Our ability to maintain customer satisfaction depends in part on the quality of our customer support. Once our Falcon platform is deployed within our customers' networks, our customers depend on our customer support services to resolve any issues relating to the implementation and maintenance of our Falcon platform. If we do not provide effective ongoing support, customer renewals and our ability to sell additional modules as part of our Falcon platform to existing customers could be adversely affected and our reputation with potential customers could be damaged. Many larger organizations have more complex networks and require higher levels of support than smaller customers and we offer premium services for these customers. Failure to maintain high- quality customer support could have a material adverse effect on our business, results of operations, and financial condition. We may need to raise additional capital to expand our operations and invest in new solutions, which capital may not be available on terms acceptable to us, or at all, and which could reduce our ability to compete and could harm our business. We expect that our existing cash and cash equivalents **and short- term investments** will be sufficient to meet our anticipated cash needs for working capital and capital expenditures for at least the next 12 months. Retaining or expanding our current levels of personnel and ~~products~~ **product and service** offerings may require additional funds to respond to business challenges, including the need to develop new products **or services** and enhancements to our Falcon platform, improve our operating infrastructure, or acquire complementary businesses and technologies. Our failure to raise additional capital or generate the significant capital necessary to expand our operations and invest in new products **or services** could reduce our ability to compete and could harm our business. Accordingly, we may need to engage in additional equity or debt financings to secure additional funds. If we raise additional equity financing, our stockholders may experience significant dilution of their ownership interests and the market price of our Class A common stock could decline. If we engage in additional debt financing, the holders of such debt would have priority over the holders of our Class A common stock, and we may be required to accept terms that further restrict our operations or our ability to incur additional indebtedness or to take other actions that would otherwise be in the interests of the debt holders. Any of the above could harm our business, results of operations, and financial condition. If we cannot maintain our company culture as we grow, we could lose the innovation, teamwork, passion, and focus on execution that we believe contribute to our success and our business may be harmed. We believe that our corporate culture has been a contributor to our success, which we believe fosters innovation, teamwork, passion and focus on building and marketing our Falcon platform. As we grow, we may find it difficult to maintain our corporate culture. Any failure to preserve our culture could harm our future success, including our ability to retain and recruit personnel, innovate and operate effectively and execute on our business strategy. Additionally, our productivity and the quality of our solutions may be adversely affected if we do not integrate and train our new employees quickly and effectively. If we experience any of these effects in connection with future growth, it could impair our ability to attract new customers, retain existing customers and expand their use of our Falcon platform, all of which would adversely affect our business, financial condition and results of operations ~~. Public health crises, such as the COVID- 19 pandemic could adversely affect our business, operating results and future revenue. We are subject to public health crises, such as the COVID- 19 pandemic, which has impacted and continues to impact worldwide economic activity and financial markets. We have previously taken and may in the future take precautionary measures intended to mitigate the spread of the COVID- 19 virus and minimize the risk to our employees, customers, partners, and the communities in which we operate to respond to developments relating to the pandemic, including developments relating to infection rates, disease variants, vaccination progress and efficacy, and evolving public health guidance. These measures could, for example, negatively affect our customer success efforts, delay and lengthen our sales~~

~~cycles, impact our sales and marketing efforts, slow our international expansion efforts, increase cybersecurity risks, and create operational or other challenges, any of which could harm our business and results of operations. In addition, public health crises may disrupt the operations of our customers and partners for an indefinite period of time. Some of our customers have been negatively impacted by the COVID- 19 pandemic, which could result in delays in accounts receivable collection, or result in decreased technology spending which could negatively affect our revenues. More generally, the COVID- 19 pandemic adversely affected economies and financial markets globally. Uncertainty caused by public health crises could lead to prolonged economic downturns, which could result in a larger customer churn than we can anticipate and reduce demand for our products and services, in which case our revenues could be significantly impacted. The lasting impact of the public health crises, including the COVID- 19 pandemic, may also exacerbate other risks discussed in this " Risk Factors " section and elsewhere in this Annual Report on Form 10- K~~ . We rely on a limited number of suppliers for certain components of the equipment we use to operate our cloud platform. Supply chain disruptions could delay our ability to expand or increase the capacity of our global data center network, replace defective equipment in our existing data centers and impact our operating costs. We rely on a limited number of suppliers for several components of the equipment we use to operate our cloud platform and provide services to our customers. We generally purchase these components on a purchase order basis, and do not have long- term contracts guaranteeing supply. Our reliance on these suppliers exposes us to risks, including reduced control over production costs and constraints based on the then current availability, terms and pricing of these components. If we experience disruption or delay from our suppliers, we may not be able to obtain supplies or components from alternative suppliers on a timely basis or on terms that are favorable to us, if at all. The technology industry has ~~recently~~ experienced widespread component shortages and delivery delays, including as a result of geopolitical tensions, **public health crises** ~~the COVID- 19 pandemic~~ and natural disasters. While we have taken steps to mitigate our supply chain risk, supply chain disruptions and delays could nevertheless adversely impact our operations by, among other things, causing us to delay opening new data centers, delay increasing capacity or replacing defective equipment at existing data centers, and experience increased operating costs. Risks Related to Intellectual Property, Legal, and Regulatory Matters The success of our business depends in part on our ability to protect and enforce our intellectual property rights. We believe our intellectual property is an essential asset of our business, and our success and ability to compete depend in part upon protection of our intellectual property rights. We rely on a combination of patent, copyright, trademark and trade secret laws, as well as confidentiality procedures and contractual provisions, to establish and protect our intellectual property rights in the United States and abroad, all of which provide only limited protection. The efforts we have taken to protect our intellectual property may not be sufficient or effective, and our trademarks, copyrights and patents may be held invalid or unenforceable. Moreover, we cannot assure you that any patents will be issued with respect to our currently pending patent applications in a manner that gives us adequate defensive protection or competitive advantages, or that any patents issued to us will not be challenged, invalidated or circumvented. We have filed for patents in the United States and in certain non- U. S. jurisdictions, but such protections may not be available in all countries in which we operate or in which we seek to enforce our intellectual property rights, or may be difficult to enforce in practice. For example, many foreign countries have compulsory licensing laws under which a patent owner must grant licenses to third parties. In addition, many countries limit the enforceability of patents against certain third parties, including government agencies or government contractors. In these countries, patents may provide limited or no benefit. Moreover, we may need to expend additional resources to defend our intellectual property rights in these countries, and our inability to do so could impair our business or adversely affect our international expansion. Our currently issued patents and any patents that may be issued in the future with respect to pending or future patent applications may not provide sufficiently broad protection or they may not prove to be enforceable in actions against alleged infringers. We may not be effective in policing unauthorized use of our intellectual property, and even if we do detect violations, litigation or technical changes to our products may be necessary to enforce our intellectual property rights. Protecting against the unauthorized use of our intellectual property rights, technology and other proprietary rights is expensive and difficult, particularly outside of the United States. Any enforcement efforts we undertake, including litigation, could be time- consuming and expensive and could divert management' s attention, which could harm our business and results of operations. Further, attempts to enforce our rights against third parties could also provoke these third parties to assert their own intellectual property or other rights against us, or result in a holding that invalidates or narrows the scope of our rights, in whole or in part. The inability to adequately protect and enforce our intellectual property and other proprietary rights could seriously harm our business, results of operations and financial condition. Even if we are able to secure our intellectual property rights, we cannot assure you that such rights will provide us with competitive advantages or distinguish our services from those of our competitors or that our competitors will not independently develop similar technology, duplicate any of our technology, or design around our patents. Claims by others that we infringe their proprietary technology or other intellectual property rights could harm our business. A number of companies in our industry hold a large number of patents and also protect their copyright, trade secret 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. ~~For example, in March 2022, Webroot, Inc. and Open Text, Inc. filed a lawsuit against us alleging that certain of our products infringe on patents held by them.~~ As we face increasing competition and grow, the possibility of intellectual property rights claims against us also grows. In addition, to the extent we hire personnel from competitors, we may be subject to allegations that such personnel have divulged proprietary or other confidential information to us. From time to time, third parties have in the past and may in the future assert claims of infringement of intellectual property rights against us. Third parties may in the future also assert claims against our customers or channel partners, whom our standard license and other agreements obligate us to indemnify against claims that our solutions infringe the intellectual property rights of third parties. As the number of products and competitors in the security and IT operations market increases and overlaps occur, claims of infringement, misappropriation, and other violations of intellectual property rights may increase. While we intend to increase the size of our patent portfolio, many of our

competitors and others may now and in the future have significantly larger and more mature patent portfolios than we have. In addition, future litigation may involve non- practicing entities, companies or other patent owners who have no relevant product offerings or revenue and against whom our own patents may therefore provide little or no deterrence or protection. Any claim of intellectual property infringement by a third party, even a claim without merit, could cause us to incur substantial costs defending against such claim, could distract our management from our business and could require us to cease use of such intellectual property. Additionally, our insurance may not cover intellectual property rights infringement claims that may be made. In the event that we fail to successfully defend ourselves against an infringement claim, a successful claimant could secure a judgment or otherwise require payment of legal fees, settlement payments, ongoing royalties or other costs or damages; or we may agree to a settlement that prevents us from offering certain services or features; or we may be required to obtain a license, which may not be available on reasonable terms, or at all, to use the relevant technology. If we are prevented from using certain technology or intellectual property, we may be required to develop alternative, non- infringing technology, which could require significant time, effort and expense and may ultimately not be successful. Additionally, we may be unable to continue to offer our affected services or features while developing such technology. Although third parties may offer a license to their technology or other intellectual property, the terms of any offered license may not be acceptable, and the failure to obtain a license or the costs associated with any license could cause our business, financial condition and results of operations to be adversely affected. In addition, some licenses may be nonexclusive, and therefore our competitors may have access to the same technology licensed to us. If a third party does not offer us a license to its technology or other intellectual property on reasonable terms, or at all, we could be enjoined from continued use of such intellectual property. As a result, we may be required to develop alternative, non- infringing technology, which could require significant time, effort and expense and may ultimately not be successful. Additionally, we may be unable to continue to offer our affected products, subscriptions or services, while developing such technology. Furthermore, a successful claimant could secure a judgment or we may agree to a settlement that prevents us from distributing certain products, providing certain subscriptions or performing certain services. Any such judgment or settlement could also require us to pay substantial damages, royalties or other fees. Any of these events could harm our business, financial condition and results of operations. We license technology from third parties, and our inability to maintain those licenses could harm our business. We currently incorporate, and will in the future incorporate, technology that we license from third parties, including software, into our solutions. We cannot be certain that our licensors do not or will not infringe on the intellectual property rights of third parties or that our licensors have or will have sufficient rights to the licensed intellectual property in all jurisdictions in which we may sell our Falcon platform. Some of our agreements with our licensors may be terminated by them for convenience, or otherwise provide for a limited term. If we are unable to continue to license technology because of intellectual property infringement claims brought by third parties against our licensors or against us, or if we are unable to continue our license agreements or enter into new licenses on commercially reasonable terms, our ability to develop and sell solutions and services containing or dependent on that technology would be limited, and our business could be harmed. Additionally, if we are unable to license technology from third parties, we may be forced to acquire or develop alternative technology, which we may be unable to do in a commercially feasible manner or at all, and may require us to use alternative technology of lower quality or performance standards. This could limit or delay our ability to offer new or competitive solutions and increase our costs. As a result, our margins, market share, and results of operations could be significantly harmed. We are required to comply with stringent, complex and evolving laws, rules, regulations and standards in many jurisdictions, as well as contractual obligations, relating to data privacy and security. Any actual or perceived failure to comply with these requirements could have a material adverse effect on our business. We are required to comply with stringent, complex and evolving laws, rules, regulations and standards in many jurisdictions, as well as contractual obligations, relating to data privacy and security. Ensuring ~~that our collection, use, transfer, storage and other processing of personal information complies~~ **compliance** with such requirements ~~can~~ **may** increase operating costs, impact **our data processing practices and policies and** the development of new products or services, and reduce operational efficiency **, any of which could adversely affect our business and operations** . In the United States, there are numerous federal, state and local data privacy and security laws, rules, and regulations governing the collection, sharing, use, retention, disclosure, security, transfer, storage and other processing of personal information, including federal and state data privacy and security laws, data breach notification laws, and data disposal laws. For example, at the federal level, we are subject to, among other laws and regulations, the rules and regulations promulgated under the authority of the Federal Trade Commission (which has the authority to regulate and enforce against unfair or deceptive acts or practices in or affecting commerce, including acts and practices with respect to data privacy and security), as well as the Electronic Communication Privacy Act, the Computer Fraud and Abuse Act, the Health Insurance Portability and Accountability Act, and the Gramm Leach Bliley Act. The United States Congress also has considered, is currently considering, and may in the future consider, various proposals for comprehensive federal data privacy and security legislation, to which we may become subject if passed. ~~If we are found to have violated applicable laws or regulations, we also may be subject to penalties, fines, damages, injunctions or other outcomes that may adversely affect our operations and financial results.~~ At the state level, we are subject to laws and regulations such as the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively, the " CCPA "). The CCPA broadly defines personal information and gives California residents expanded privacy rights and protections, such as affording them the right to access and request deletion of their information and to opt out of certain sharing and sales of personal information ~~. The CCPA also prohibits covered businesses from discriminating against California residents for exercising any of their CCPA rights~~ . The CCPA provides for severe civil penalties and statutory damages for violations and a private right of action for certain data breaches that result in the loss of unencrypted personal information. This private right of action is expected to increase the likelihood of, and risks associated with, data breach litigation. Numerous other states have also enacted, or are in the process of enacting or considering, comprehensive state- level data privacy and security laws, rules, and regulations that share similarities with the CCPA ~~. At least~~

~~four such laws, in Virginia, Colorado, Connecticut, and Utah, have taken effect, or are scheduled to take effect, in 2023~~ . Moreover, laws in all 50 U. S. states require businesses to provide notice under certain circumstances to consumers whose personal information has been disclosed as a result of a data breach ~~. These state statutes, and other similar state or federal laws that may be enacted in the future, may require us to modify our data processing practices and policies, incur substantial compliance- related costs and expenses, and otherwise suffer adverse impacts on our business~~ . Internationally, virtually every jurisdiction in which we operate has established its own data privacy and security legal framework with which we must comply. For example, we are required to comply with the European Union (" EU ") General Data Protection Regulation (" GDPR ") **and its equivalent in the U. K. (" U. K. GDPR ")** , which ~~imposes~~ **impose** stringent obligations regarding the collection, control, use, sharing, disclosure and other processing of personal data ~~. Additionally, following the United Kingdom' s withdrawal from the EU, we also are subject to the U. K. General Data Protection Regulation (" U. K. GDPR "), a version of the GDPR as implemented into the laws of the United Kingdom (" U. K. ")~~ . While the GDPR and U. K. GDPR remain substantially similar for the time being, the U. K. government has announced that it would seek to chart its own path on data protection and reform its relevant laws, including in ways that may differ from the GDPR. While these developments increase uncertainty with regard to data protection regulation in the U. K., even in their current, substantially similar form, the GDPR and U. K. GDPR can expose businesses to divergent parallel regimes that may be subject to potentially different interpretations and enforcement actions for certain violations and related uncertainty. Failure to comply with the GDPR or the U. K. GDPR can result in significant fines and other liability, including, under the GDPR, fines of up to EUR 20 million (or GBP 17. 5 million under the U. K. GDPR) or four percent (4 %) of annual global revenue, whichever is greater. ~~The cost of compliance, and the potential~~ **European data protection authorities have already imposed fines** for ~~fines and penalties for non- compliance, with~~ GDPR **violations of up to, in some cases, hundreds of millions of Euros** ~~and U. K. GDPR may have a significant adverse effect on our business and operations~~ . Legal developments in the European Economic Area (" EEA ") ~~, including recent rulings from the Court of Justice of the European Union (" CJEU ") and from various EU member state data protection authorities,~~ have created complexity and uncertainty regarding processing and transfers of personal data from the EEA to the United States and other so-called third countries outside the EEA, including in the context of website cookies. Similar complexities and uncertainties also apply to transfers from the U. K. to third countries. While we have taken steps to mitigate the impact on us, such as implementing the European Commission' s standard contractual clauses (" SCCs ") **and the U. K.' s international Data Transfer Agreement (or the U. K.' s international data transfer addendum that can be used with the SCCs)** , the efficacy and longevity of these mechanisms remains uncertain. ~~Moreover~~ **On July 10** , ~~in 2021~~ **2023** , the European Commission adopted ~~new SCCs, which impose on companies additional obligations relating to~~ **an adequacy decision concluding that the U. S. ensures an adequate level of protection for** personal data ~~transfers~~ **transferred from** ~~out of~~ the **EU** ~~EEA, including the obligation~~ to ~~update internal~~ **the U. S. under the recently adopted EU- U. S. Data** ~~privacy~~ **Privacy** ~~practices~~ **Framework (followed on October 12** , ~~conduct transfer impact assessments~~ **2023 with the adoption of** ~~and~~ **an adequacy decision in the U** ~~, as required, implement additional security measures~~ . ~~The~~ **K. for the U. K.- U. S. Data Bridge); however, such** new **adequacy decision** ~~SCCs may increase the legal risks and liabilities under EU laws associated with cross- border data transfers, and result in material increased compliance and operational costs. While the European Commission announced in March 2022 that an agreement in principle had been reached between EU and U. S. authorities regarding a new transatlantic data privacy framework, no formal agreement~~ has been ~~finalized~~ **challenged in EU courts** , and ~~any such agreement, if formalized,~~ is likely to face **additional** ~~challenge~~ **challenges** ~~at the CJEU~~ . Moreover, although the U. K. currently has an adequacy decision from the European Commission, such that SCCs are not required for the transfer of personal data from the EEA to the U. K., that decision will sunset in June 2025 unless extended and it may be revoked in the future by the European Commission if the U. K. data protection regime is reformed in ways that deviate substantially from the GDPR ~~. Adding further complexity for international data flows, in March 2022, the U. K. adopted its own International Data Transfer Agreement (" IDTA ") for transfers of personal data out of the U. K. to so- called third countries, as well as an international data transfer addendum (U. K. Addendum) that can be used with the SCCs for the same purpose~~ . The EU has also proposed legislation that would regulate non- personal data and establish new cybersecurity standards, and other countries, including the U. K., may similarly do so in the future. If we are otherwise unable to transfer data, including personal data, between and among countries and regions in which we operate, it could affect the manner in which we provide our services, the geographical location or segregation of our relevant systems and operations, and could adversely affect our financial results. While we have implemented new controls and procedures designed to comply with the requirements of the GDPR, U. K. GDPR and the data privacy and security laws of other jurisdictions in which we operate, such procedures and controls may not be effective in ensuring compliance or preventing unauthorized transfers of personal data. Moreover, while we strive to publish and prominently display privacy policies that are accurate, comprehensive, and compliant with applicable laws, rules regulations and industry standards, we cannot ensure that our privacy policies and other statements regarding our practices will be sufficient to protect us from claims, proceedings, liability or adverse publicity relating to data privacy and security. Although we endeavor to comply with our privacy policies, we may at times fail to do so or be alleged to have failed to do so. If our public statements about our use, collection, disclosure and other processing of personal information, whether made through our privacy policies, information provided on our website, press statements or otherwise, are alleged to be deceptive, unfair or misrepresentative of our actual practices, we may be subject to potential government or legal investigation or action, including by the Federal Trade Commission or applicable state attorneys general. Our compliance efforts are further complicated by the fact that data privacy and security laws, rules, regulations and standards around the world are rapidly evolving, may be subject to uncertain or inconsistent interpretations and enforcement, and may conflict among various jurisdictions. Any failure or perceived failure by us to comply with our privacy policies, or applicable data privacy and security laws, rules, regulations, standards, certifications or contractual obligations, or any compromise of security that results in unauthorized access to, or unauthorized loss, destruction, use, modification, acquisition,

disclosure, release or transfer of personal information, may result in requirements to modify or cease certain operations or practices, the expenditure of substantial costs, time and other resources, proceedings or actions against us, legal liability, governmental investigations, enforcement actions, claims, fines, judgments, awards, penalties, sanctions and costly litigation (including class actions). **There also has been increased regulatory scrutiny from the SEC with respect to adequately disclosing risks concerning cybersecurity and data privacy. Such scrutiny from the SEC increases the risk of investigations into the cybersecurity practices, and related disclosures, of companies within its jurisdiction.** Any of the foregoing could harm our reputation, distract our management and technical personnel, increase our costs of doing business, adversely affect the demand for our products and services, and ultimately result in the imposition of liability, any of which could have a material adverse effect on our business, financial condition and results of operations. 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 negatively impact our ability to contract with customers, including those in the public sector. Our business is subject to regulation by various federal, state, local and foreign governmental agencies, including agencies responsible for monitoring and enforcing data protection, data privacy and data security laws and regulations, employment and labor laws, workplace safety, product safety, environmental laws, consumer protection laws, anti- bribery laws, import and export controls, federal securities laws and tax laws and regulations. In certain jurisdictions, these regulatory requirements may be more stringent than in the United States **. Increased scrutiny of technologies like AI may also become subject to regulation under new laws or new applications of existing laws, such as the AI Act being considered in the EU** . Noncompliance by us, our employees, representatives, contractors, channel partners, agents, intermediaries, or other third parties with applicable regulations or requirements could subject us to: • investigations, enforcement actions and sanctions; • mandatory changes to our Falcon platform; • 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; • loss of our license to do business in the jurisdictions in which we operate; 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 management' s attention and resources and an increase in professional fees. Enforcement actions and sanctions could harm our business, results of operations and financial condition. We endeavor to properly classify employees as exempt versus non- exempt under applicable law. Although there are no pending or threatened material claims or investigations against us asserting that some employees are improperly classified as exempt, the possibility exists that some of our current or former employees could have been incorrectly classified as exempt employees. These laws and regulations impose added costs on our business, and failure by us, our employees, representatives, contractors, channel partners, agents, intermediaries, or other third parties to comply with these or other applicable regulations and requirements could lead to claims for damages, penalties, termination of contracts, loss of exclusive rights in our intellectual property and temporary suspension or permanent debarment from government contracting. Any such damages, penalties, disruptions or limitations in our ability to do business with customers, including those in the public sector, could result in reduced sales of our products **or services** , substantial product inventory write- offs, reputational damage, penalties, and other sanctions, any of which could harm our business, reputation, and results of operations. We are subject to ~~laws and regulations, including~~ governmental export ~~and import~~ controls ~~,~~ **and economic** sanctions ~~, and anti- corruption~~ laws ~~,~~ that could impair our ability to compete in ~~our~~ **international** markets and subject us to liability if we are not in full compliance with applicable laws. ~~We~~ **Our products, services and business activities, including our collection of information about cyber threats,** are subject to ~~laws and regulations, including governmental~~ **various restrictions under U. S.** export controls **and trade and economic sanctions laws** , **including the** ~~that could subject us to liability or impair our ability to compete in our markets. Our products are subject to~~ U. S. **Commerce** ~~export controls, including the U. S.~~ Department ~~of Commerce~~ ' s Export Administration Regulations ~~,~~ and ~~we and our employees, representatives, contractors, agents, intermediaries, and other third parties are also subject to various~~ economic and trade sanctions regulations ~~administered~~ **maintained** by the U. S. Treasury Department' s Office of Foreign Assets Control. **The** ~~We incorporate standard encryption algorithms into our products, which, along with the underlying technology, may be exported outside of the U. S. only with the required export authorizations, including by license, license exception or other appropriate government authorizations, which may require the filing of an encryption registration and classification request. Furthermore,~~ U. S. export control laws and **U. S.** economic sanctions **laws include** ~~prohibit~~ **prohibitions on** the ~~shipment~~ **sale or supply** of certain **products and services** ~~cloud- based solutions~~ to **U. S. embargoed or sanctioned** countries, governments, ~~and~~ persons **and entities and** ~~targeted by U. S. sanctions. We~~ also **require authorization for** ~~collect information about cyber threats from open sources, intermediaries, and third parties, which we use and make available to our customers in our threat industry publications. Although we take precautions and have implemented certain procedures to prevent our information collection practices and services from being provided in violation of applicable laws and regulations, our information collection practices and services may have been in~~ the **export** ~~past, and could in the future be, provided in violation~~ of **encryption items** ~~such laws and regulations~~ . In addition, ~~we cannot assure you that third parties, many of whom we do not control, have complied with all such laws or regulations. Failure by our employees, representatives, contractors, agents, intermediaries, or other third parties to comply with such laws and regulations in the collection of this information could adversely affect us, through reputational harm, loss of access to certain markets, government investigations, and civil and criminal penalties. Various~~ **various** countries regulate the import of certain encryption technology, including through import ~~permit~~ and ~~license~~ **licensing** requirements, and have enacted laws that could limit our ability to distribute our products or **service or** could limit our customers' ability to implement our ~~products~~ **service** in those countries. ~~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.~~ Changes in our products or **services or** changes in ~~export~~ **these laws** and ~~import~~ regulations may create delays in the introduction of our

products **or services** into international markets, prevent our customers with international operations from deploying our products **or services** globally or, in some cases, prevent the export or import of our products **or services** to certain countries, governments or persons altogether ~~. Any change in export or import regulations, economic sanctions or related legislation, shift in the enforcement or scope of existing regulations, or change in the countries, governments, persons or technologies targeted by such regulations, could result in decreased use of our products by, or in our decreased ability to export or sell our products to, existing or potential customers with international operations~~ . Any decreased use of our products or **services or** limitation on our ability to export **to** or sell our products **or services in international markets** would likely adversely affect our business, ~~results of operations, and~~ financial condition **, and operating results. 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. If we fail to comply with these 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 monetary penalties. Although we take precautions to prevent our products or services from being provided in violation of such laws, our products or services may have been in the past, and could in the future be, provided in violation of such laws, despite the precautions we take. This could result in negative consequences to us, including government investigations, penalties and harm to our reputation** . We are ~~also~~ subject to **anti- corruption, anti- bribery and similar laws, and non- compliance 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, as amended (“** FCPA **”)** , the **U. K.** Bribery Act ~~,~~ **2010** and other anti- corruption, ~~sanctions,~~ 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 **in recent years** and are interpreted broadly ~~,~~ **and** prohibit companies and their employees ~~,~~ **and** agents ~~, intermediaries, and other third parties~~ from promising, authorizing, making or offering improper payments or other benefits to government officials and others in the private sector. **As we increase our international sales** ~~We leverage third parties, including intermediaries, agents,~~ and **business, our risks under these laws may increase. In addition, we use** channel partners, **agents and** ~~to conduct our business in the~~ **other** ~~U. S. and abroad, to sell subscriptions to our Falcon platform and to collect information about cyber threats. We and these~~ third- **parties to sell our products or conduct business on our behalf. We or such third** parties may have direct or indirect interactions with officials and employees of government agencies or state- owned or affiliated entities and **under certain circumstances** we ~~may~~ **could** be held liable for the corrupt or other illegal activities of **such** ~~these third- party business~~ partners ~~and intermediaries~~ , **and** our employees, representatives, contractors, ~~channel~~ partners, **and** agents ~~, intermediaries, and other third parties~~ , even if we do not **explicitly** authorize such activities. **We** ~~While we~~ have ~~policies~~ **implemented** ~~and~~ - **an** ~~procedures to address compliance with the FCPA, the Bribery Act and other~~ anti- corruption **compliance program but cannot ensure that all our employees and agents** , **as well as those companies to which we outsource certain of our business operations, will not take** ~~sanctions~~ -- **actions in violation of our policies and applicable law, for which we may be ultimately held responsible. Noncompliance with the FCPA, other applicable anti- corruption** , anti- bribery, **or** anti- money laundering ~~and similar laws, we cannot assure you that they will be effective, or that all of our employees, representatives, contractors, channel partners, agents, intermediaries, or other third parties have taken, or will not take actions, in violation of our policies and applicable law, for which we may be ultimately held responsible. As we increase our international sales and business, our risks under these laws may increase. Noncompliance with these~~ laws could subject us to investigations, **whistleblower complaints, sanctions, settlements, prosecution, and other enforcement actions within the U. S. and internationally. Any violation of these laws could result in disgorgement of profits, significant fines, damages, other civil and criminal penalties or injunctions, adverse media coverage, loss of export privileges,** severe criminal or civil sanctions ~~, settlements, prosecution, loss of export privileges~~ , suspension or debarment from U. S. government contracts ~~, other enforcement actions, disgorgement of profits, significant fines, damages, other civil and criminal penalties or injunctions, whistleblower complaints, adverse media coverage~~ and other consequences ~~. Any investigations~~ , ~~actions or sanctions~~ **any of which** could ~~harm~~ **have a material adverse effect on** our reputation, business, results of operations **,** and financial condition. Some of our technology incorporates “ open source ” software, which could negatively affect our ability to sell our Falcon platform and subject us to possible litigation. Our products and subscriptions contain third- party open source software components, and failure to comply with the terms of the underlying open source software licenses could restrict our ability to sell our products and subscriptions. The use and distribution of open source software may entail greater risks than the use of third- party commercial software, as open source licensors generally do not provide warranties or other contractual protections regarding infringement claims or the quality of the code and they can change the license terms on which they offer the open source software. Many of the risks associated with use of open source software cannot be eliminated and could negatively affect our business. In addition, the wide availability of source code used in our solutions could expose us to security vulnerabilities. Some open source licenses contain requirements that we make available source code for modifications or derivative works we create based upon the type of open source software we use. If we combine our proprietary software with open source software in a certain manner, we could, under certain open source licenses, be required to release the source code of our proprietary software to the public, including authorizing further modification and redistribution, or otherwise be limited in the licensing of our services, each of which could provide an advantage to our competitors or other entrants to the market, create security vulnerabilities in our solutions, require us to re- engineer all or a portion of our Falcon platform, and could reduce or eliminate the value of our services. This would allow our competitors to create similar products with lower development effort and time and ultimately could result in a loss of sales for us. The terms of many open source licenses have not been interpreted by U. S. courts, and there is a risk that these licenses could be construed in ways that could impose unanticipated conditions or restrictions on our ability to commercialize products and subscriptions incorporating such software. Moreover, we cannot assure you that our processes for controlling our use of open source software in our products and subscriptions will be effective. From time to time, we may face claims from third

parties asserting ownership of, or demanding release of, the open source software or derivative works that we developed using such software (which could include our proprietary source code), or otherwise seeking to enforce the terms of the applicable open source license. These claims could result in litigation. Litigation could be costly for us to defend, have a negative effect on our results of operations and financial condition or require us to devote additional research and development resources to change our solutions. Responding to any infringement or noncompliance claim by an open source vendor, regardless of its validity, discovering certain open source software code in our Falcon platform, or a finding that we have breached the terms of an open source software license, could harm our business, results of operations and financial condition, by, among other things: • resulting in time- consuming and costly litigation; • diverting management' s time and attention from developing our business; • requiring us to pay monetary damages or enter into royalty and licensing agreements that we would not normally find acceptable; • causing delays in the deployment of our Falcon platform or service offerings to our customers; • requiring us to stop offering certain services or features of our Falcon platform; • requiring us to redesign certain components of our Falcon platform using alternative non- infringing or non- open source technology, which could require significant effort and expense; • requiring us to disclose our software source code and the detailed program commands for our software; and • requiring us to satisfy indemnification obligations to our customers. We **utilize Artificial Intelligence, which could expose us to liability or adversely affect our business. We incorporate novel uses of AI technologies, including generative AI, into our products and operations. AI is complex and rapidly evolving, and we face significant competition from other companies as well as an evolving regulatory landscape. The introduction of AI into new or existing products may result in new or enhanced governmental or regulatory scrutiny, litigation, confidentiality, ethical concerns, or other complications that could adversely affect our business, reputation, or financial results. For example, if we do not have sufficient rights to use the data or other material or content on which our AI technologies rely, we may incur liability through the violation of applicable laws, third- party intellectual property, privacy or other rights, or contracts to which we are a party. AI algorithms may be flawed, insufficient, of poor quality, reflect unwanted forms of bias, or contain other errors or inadequacies, any of which may not be easily detectable. Our customers or others may rely on or use this flawed content to their detriment, which may expose us to brand or reputational harm, competitive harm, and / or legal liability. The use of AI presents emerging ethical and social issues, and if we enable or offer solutions that draw scrutiny or controversy due to their perceived or actual impact on customers or on society as a whole, we may experience brand or reputational harm, competitive harm, and / or legal liability. The technologies underlying AI and its uses are subject to a variety of laws, including intellectual property, privacy, data protection and cybersecurity, consumer protection, competition, and equal opportunity laws, and are expected to be subject to increased regulation and new laws or new applications of existing laws. AI is the subject of ongoing review by various U. S. governmental and regulatory agencies, and various U. S. states and other foreign jurisdictions are applying, or are considering applying, their cybersecurity and data protection laws to AI or are considering general legal frameworks for AI, such as the AI Act currently being considered in the EU. As a fast- evolving and complicated technology subject to significant government attention, AI- related legislation and regulation may be developed and apply to AI in unexpected ways. We may not be able to anticipate how to respond to or comply with these rapidly evolving frameworks, and we may need to expend resources to adjust our offerings in certain jurisdictions if the legal frameworks are inconsistent across jurisdictions. Furthermore, because AI technology itself is highly complex and rapidly developing, it is not possible to predict all of the legal, operational or technological risks that may arise relating to the use of AI. We** provide service level commitments under some of our customer contracts. If we fail to meet these contractual commitments, we could be obligated to provide credits for future service and our business could suffer. Certain of our customer agreements contain service level commitments, which contain specifications regarding the availability and performance of our Falcon platform. Any failure of or disruption to our infrastructure could impact the performance of our Falcon platform and the availability of services to customers. If we are unable to meet our stated service level commitments or if we suffer extended periods of poor performance or unavailability of our Falcon platform, we may be contractually obligated to provide affected customers with service credits for future subscriptions, and, in certain cases, refunds. To date, there has not been a material failure to meet our service level commitments, and we do not currently have any material liabilities accrued on our balance sheets for such commitments. 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 with our customers. We are currently, and may in the future become, involved in litigation that may adversely affect us. We are regularly subject to claims, suits, and government investigations and other proceedings including patent, product liability, class action, whistleblower, personal injury, property damage, labor and employment (including allegations of wage and hour violations), commercial disputes, compliance with laws and regulatory requirements and other matters, and we may become subject to additional types of claims, suits, investigations and proceedings as our business develops. Such claims, suits, and government investigations and proceedings are inherently uncertain and their results cannot be predicted with certainty. Regardless of the outcome, any of these types of legal proceedings can have an adverse impact on us because of legal costs and diversion of management attention and resources, and could cause us to incur significant expenses or liability, adversely affect our brand recognition, and / or require us to change our business practices. The expense of litigation and the timing of this expense from period to period are difficult to estimate, subject to change and could adversely affect our results of operations. It is possible that a resolution of one or more such proceedings could result in substantial damages, settlement costs, fines and penalties that could adversely affect our business, consolidated financial position, results of operations, or cash flows in a particular period. These proceedings could also result in reputational harm, sanctions, consent decrees, or orders requiring a change in our business practices. Because of the potential risks, expenses and uncertainties of litigation, we may, from time to time, settle disputes, even where we have meritorious claims or defenses, by agreeing to settlement agreements. Because litigation is inherently unpredictable, we cannot assure you that the results of any of

these actions will not have a material adverse effect on our business, financial condition, results of operations, and prospects. Any of these consequences could adversely affect our business and results of operations. Our business is subject to the risks of warranty claims, product returns, product liability, and product defects from real or perceived defects in our solutions or their misuse by our customers or third parties and indemnity provisions in various agreements potentially expose us to substantial liability for intellectual property infringement and other losses. We may be subject to liability claims for damages related to errors or defects in our solutions. A material liability claim or other occurrence that harms our reputation or decreases market acceptance of our products may harm our business and results of operations. Although we generally have limitation of liability provisions in our terms and conditions of sale, these provisions do not cover our indemnification obligations ~~as described in the section titled " Management' s Discussion and Analysis of Financial Condition and Results of Operations — Indemnification "~~ and they may not fully or effectively protect us from claims as a result of federal, state, or local laws or ordinances, or unfavorable judicial decisions in the United States or other countries. The sale and support of our products also entails the risk of product liability claims. Additionally, our agreements with customers and other third parties typically 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 regarding intellectual property infringement, breach of agreement, including confidentiality, privacy and security obligations, violation of applicable laws, damages caused by failures of our solutions or to property or persons, or other liabilities relating to or arising from our products and services, or other acts or omissions. These contractual provisions often survive termination or expiration of the applicable agreement. We have not to date received any indemnification claims from third parties. However, as we continue to grow, the possibility of these claims against us will increase. If our customers or other third parties we do business with make intellectual property rights or other indemnification claims against us, we will incur significant legal expenses and may have to pay damages, license fees, and / or stop using technology found to be in violation of the third party' s rights. We may also have to seek a license for the technology. Such 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 solutions or features. We may also be required to develop alternative non- infringing technology, which could require significant effort and expense and / or cause us to alter our products and services, which could harm our business. Large indemnity obligations, whether for intellectual property or other claims, could harm our business, results of operations, and financial condition. Additionally, our Falcon platform may be used by our customers and other third parties who obtain access to our solutions for purposes other than for which our platform was intended. For example, our Falcon platform might be misused by a customer to monitor its employee' s activities in a manner that violates the employee' s privacy rights under applicable law. During the course of performing certain solution- related services and our professional services, our teams may have significant access to our customers' networks. We cannot be sure that an employee may not take advantage of such access which may make our customers vulnerable to malicious activity by such employee. Any such misuse of our Falcon platform could result in negative press coverage and negatively affect our reputation, which could result in harm to our business, reputation, and results of operations. We maintain insurance to protect against certain claims associated with the use of our products, but our insurance coverage may not adequately cover any claim asserted against us. In addition, even claims that ultimately are unsuccessful could result in our expenditure of funds in litigation, divert management' s time and other resources, and harm our business and reputation. We offer our Falcon Complete customers a limited warranty, subject to certain conditions. While we maintain insurance relating to our warranty, we cannot be certain that our insurance coverage will be adequate to cover such claims, that such insurance will continue to be available to us on commercially reasonable terms, or at all, or that any insurer will not deny coverage as to any claim. Any failure or refusal of our insurance providers to provide the expected insurance benefits to us after we have paid the warranty claims would cause us to incur significant expense or cause us to cease offering this warranty which could damage our reputation, cause us to lose customers, expose us to liability claims by our customers, negatively impact our sales and marketing efforts, and have an adverse effect on our business, financial condition and results of operations. Risks Related to Ownership of Our Class A Common Stock The market price of our Class A common stock may be volatile regardless of our operating performance, and you could lose all or part of your investment. We cannot predict the prices at which our Class A common stock will trade. The market price of our Class A common stock depends on a number of factors, including those described in this " Risk Factors " section, many of which are beyond our control and may not be related to our operating performance. These fluctuations could cause you to lose all or part of your investment in our Class A common stock. Factors that could cause fluctuations in the market price of our Class A common stock include the following: • actual or anticipated changes or fluctuations in our results of operations; • the financial projections we may provide to the public, any changes in these projections or our failure to meet these projections; • announcements by us or our competitors of new products or **services or** new or terminated significant contracts, commercial relationships or capital commitments; • industry or financial analyst or investor 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; • price and volume fluctuations in the overall stock market from time to time; • changes in operating performance and stock market valuations of other technology companies generally, or those in our industry in particular; • failure of industry or financial analysts to maintain coverage of us, changes in financial estimates by any analysts who follow our company, or our failure to meet these estimates or the expectations of investors; • actual or anticipated developments in our business or our competitors' businesses or the competitive landscape generally; • litigation involving us, our industry or both, or investigations by regulators into our operations or those of our competitors; • developments or disputes concerning our intellectual property rights or our solutions, or third- party proprietary rights; • announced or completed acquisitions of businesses or technologies by us or our competitors; • new laws or regulations or new interpretations of existing laws or regulations applicable to our business; • any major changes in our management or our board of directors, particularly with respect to Mr. Kurtz; • effects of public health crises, pandemics and epidemics ~~, such as COVID- 19~~ ; • general economic conditions and slow or negative growth of our markets; and • other events or factors, including

those resulting from war, incidents of terrorism or responses to these events. In addition, the stock market in general, and the market for technology companies in particular, has experienced extreme price and volume fluctuations that have often been unrelated or disproportionate to the operating performance of those companies. Broad market and industry factors may seriously affect the market price of our Class A common stock, regardless of our actual operating performance. In addition, in the past, following periods of volatility in the overall market and the market prices of a particular company' s securities, securities class action litigation has often been instituted against that company. Securities litigation, if instituted against us, could result in substantial costs and divert our management' s attention and resources from our business. This could have an adverse effect on our business, results of operations and financial condition. Sales of substantial amounts of our Class A common stock in the public markets, or the perception that they might occur, could reduce the price that our Class A common stock might otherwise attain and may dilute your voting power and your ownership interest in us. Sales of a substantial number of shares of our Class A common stock in the public market, including shares of Class A stock that have been converted from shares of Class B common stock, and particularly sales by our directors, executive officers and significant stockholders, or the perception that these sales could occur, could adversely affect the market price of our Class A common stock. As of February ~~28~~ **29**, ~~2023~~ **2024**, we had ~~222~~ **229**, ~~937~~ **383**, ~~242~~ **465** shares of Class A common stock outstanding and 12, ~~926~~ **485**, ~~743~~ **193** shares of Class B common stock outstanding. In addition, certain holders of our Class B common stock are entitled to rights with respect to registration of these shares under the Securities Act pursuant to our amended and restated registration rights agreement. If these holders of our Class B common stock, by exercising their registration rights, sell a large number of shares, they could adversely affect the market price for our Class A common stock. We may also issue our shares of Class A common stock or securities convertible into shares of our Class A common stock from time to time in connection with a financing, acquisition, investments or otherwise. Any such issuance could result in substantial dilution to our existing stockholders and cause the market price of our Class A common stock to decline. If industry or financial analysts do not publish research or reports about our business, or if they issue inaccurate or unfavorable research regarding our Class A common stock, our stock price and trading volume could decline. The trading market for our Class A common stock will be influenced by the research and reports that industry or financial analysts publish about us or our business. We do not control these analysts or the content and opinions included in their reports. If any of the analysts who cover us issues an inaccurate or unfavorable opinion regarding our stock price, our stock price would likely decline. In addition, the stock prices of many companies in the technology industry have declined significantly after those companies have failed to meet, or significantly exceed, the financial guidance publicly announced by the companies or the expectations of analysts. If our financial results fail to meet, or significantly exceed, our announced guidance or the expectations of analysts or public investors, analysts could downgrade our Class A common stock or publish unfavorable research about us. If one or more of these analysts cease coverage of our company or fail to publish reports on us regularly, our visibility in the financial markets could decrease, which in turn could cause our stock price or trading volume to decline. The dual class structure of our common stock has the effect of concentrating voting control with those stockholders who held our capital stock (or options or other securities convertible into or exercisable for our capital stock) prior to the completion of our initial public offering, including our executive officers, employees, directors, principal stockholders, and their affiliates, which will limit your ability to influence the outcome of matters submitted to our stockholders for approval. Our Class B common stock has 10 votes per share, and our Class A common stock has one vote per share. The dual class structure of our common stock has the effect of concentrating voting control with those stockholders who held our capital stock (or options or other securities convertible into or exercisable for our capital stock) prior to our initial public offering, including our executive officers, employees, directors, principal stockholders, and their affiliates, which will limit your ability to influence the outcome of matters submitted to our stockholders for approval, including the election of our directors and the approval of any change in control transaction. Future transfers by holders of Class B common stock will generally result in those shares converting to Class A common stock, which will have the effect, over time, of increasing the relative voting power of those holders of Class B common stock who retain their shares in the long term. As of January 31, ~~2023~~ **2024**, our executive officers, directors, one of our current stockholders and its respective affiliates held, in aggregate, ~~38~~ **36** % of the voting power of our outstanding capital stock. As a result, these stockholders, acting together, have control over most matters that require approval by our stockholders, including the election of directors and approval of significant corporate transactions. They may also have interests that differ from yours and may vote in a way with which you disagree and which may be adverse to your interests. This concentration of ownership may have the effect of delaying, preventing or deterring a change of control or other liquidity event of our company, could deprive our stockholders of an opportunity to receive a premium for their shares of common stock as part of a sale or other liquidity event and might ultimately affect the market price of our common stock. Further, our amended and restated certificate of incorporation provides that, to the fullest extent permitted by law, the doctrine of " corporate opportunity " does not apply to Accel, or its respective affiliates, in a manner that would prohibit them from investing in competing businesses or doing business with our partners or customers. We do not intend to pay dividends in the foreseeable future. As a result, your ability to achieve a return on your investment will depend on appreciation in the price of our Class A common stock. We have never declared or paid any cash dividends on our capital stock. We currently intend to retain all available funds and any future earnings for use in the operation of our business and do not anticipate paying any dividends in the foreseeable future. Any determination to pay dividends in the future will be at the discretion of our board of directors. Additionally, our ability to pay dividends is limited by restrictions on our ability to pay dividends or make distributions under the terms of our credit facility. Accordingly, investors must rely on sales of their Class A common stock after price appreciation, which may never occur, as the only way to realize any future gains on their investments. Certain provisions in our charter documents and under Delaware law could make an acquisition of our company more difficult, limit attempts by our stockholders to replace or remove members of our board of directors or current management, and may adversely affect the market price of our Class A common stock. Our amended and restated certificate of incorporation and amended and restated bylaws contain provisions that could delay or

prevent a change in control of our company. These provisions could also make it difficult for stockholders to elect directors that are not nominated by the current members of our board of directors or take other corporate actions, including effecting changes in our management. These provisions include: • our dual class common stock structure, which provides our holders of Class B common stock 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 and Class B common stock; • a classified board of directors with three- year staggered terms, which could delay the ability of stockholders to change the membership of a majority of our board of directors; • the ability of our board of directors to issue shares of preferred stock and to determine the price and other terms of those shares, including preferences and voting rights, without stockholder approval, which could be used to significantly dilute the ownership of a hostile acquirer; • the exclusive right of our board of directors to elect a director to fill a vacancy created by the expansion of our board of directors or the resignation, death or removal of a director, which prevents stockholders from being able to fill vacancies on our board of directors; • a prohibition on stockholder action by written consent, which forces stockholder action to be taken at an annual or special meeting of our stockholders, which prohibition will take effect on the first date on which the number of outstanding shares of our Class B common stock represents less than 10 % of the aggregate number of outstanding shares of our Class A common stock and our Class B common stock, taken together as a single class; • the requirement that a special meeting of stockholders may be called only by the chairperson of our board of directors, chief executive officer or by the board of directors acting pursuant to a resolution adopted by a majority of our board of directors, which could delay the ability of our stockholders to force consideration of a proposal or to take action, including the removal of directors; • certain amendments to our amended and restated certificate of incorporation require the approval of two-thirds of the then- outstanding voting power of our capital stock; and • advance notice procedures with which stockholders must comply to nominate candidates to our board of directors or to propose matters to be acted upon at a stockholders' meeting, which may discourage or deter a potential acquirer from conducting a solicitation of proxies to elect the acquirer' s own slate of directors or otherwise attempting to obtain control of us. These provisions may prohibit large stockholders, in particular those owning 15 % or more of our outstanding voting stock, from merging or combining with us for a certain period of time. Our amended and restated bylaws provide that the Court of Chancery of the State of Delaware, and to the extent enforceable, the federal district courts of the United States, will be the exclusive forum for certain disputes between us and our stockholders, which could limit our stockholders' ability to obtain a favorable 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 exclusive forum for: • any derivative action or proceeding brought on our behalf; • any action asserting a breach of fiduciary duty; • any action asserting a claim against us arising under the Delaware General Corporation Law, our amended and restated certificate of incorporation or our amended and restated bylaws; • any action to interpret, apply, enforce or determine the validity of our amended and restated certificate of incorporation or our amended and restated bylaws; and • any action asserting a claim against us that is governed by the internal- affairs doctrine. However, this exclusive forum provision does not apply to suits brought to enforce a duty or liability created by the Exchange Act. In addition, our amended and restated bylaws provide that the federal district courts of the United States will be the exclusive forum for resolving any complaint asserting a cause of action arising under the Securities Act, subject to and contingent upon a final adjudication in the State of Delaware of the enforceability of such exclusive forum provision. These exclusive- forum provisions may limit a stockholder' s ability to bring a claim in a judicial forum that it finds favorable for disputes with us or our directors, officers or other employees, which may discourage lawsuits against us and our directors, officers and other employees. Risks Related to our Indebtedness Our indebtedness could adversely affect our financial condition. As of January 31, ~~2023~~ **2024** , we had $ 750. 0 million principal amount of indebtedness outstanding (excluding intercompany indebtedness), and there is additional availability under our revolving facility of up to $ 750. 0 million (excluding issued but undrawn letters of credit). Our indebtedness could have important consequences, including: • limiting our ability to obtain additional financing to fund future working capital, capital expenditures, acquisitions or other general corporate requirements; • requiring a portion of our cash flows to be dedicated to debt service payments instead of other purposes, thereby reducing the amount of cash flows available for working capital, capital expenditures, acquisitions and other general corporate purposes; • increasing our vulnerability to adverse changes in general economic, industry and competitive conditions; and • exposing us to the risk of increased interest rates as certain of our borrowings, including borrowings under our revolving facility, are at variable rates of interest; and increasing our cost of borrowing. We may not be able to generate sufficient cash to service all of our indebtedness, including the notes, and may be forced to take other actions to satisfy our obligations under our indebtedness, which may not be successful. Our ability to make scheduled payments on or to refinance our debt obligations, including the Senior Notes, depends on our financial condition and results of operations, which in turn are subject to prevailing economic and competitive conditions and to certain financial, business and other factors beyond our control. We may not be able to maintain a level of cash flows from operating activities sufficient to permit us to pay the principal, premium, if any, and interest on our indebtedness, including the notes. If our cash flows and capital resources are insufficient to fund our debt service obligations, we could face substantial liquidity problems and may be forced to reduce or delay investments and capital expenditures, or to sell assets, seek additional capital or restructure or refinance our indebtedness, including the Senior Notes. Our ability to restructure or refinance our debt will depend on, among other things, the condition of the capital markets and our financial condition at such time. Any refinancing of our debt could be at higher interest rates and may require us to comply with more onerous covenants, which could further restrict our business operations. The terms of existing or future debt instruments and the indenture that governs the Senior Notes may restrict us from adopting some of these alternatives. In addition, any failure to make payments of interest and principal on our outstanding indebtedness on a timely basis would likely result in a reduction of our credit rating, which could harm our ability to incur additional indebtedness. In the absence of such cash flows and resources, we could face substantial liquidity problems and might be required to dispose of material assets or operations to meet our debt service and other obligations. Further, our credit agreement contains provisions

that restrict our ability to dispose of assets and use the proceeds from any such disposition. We may not be able to consummate those dispositions or to obtain the proceeds that we could realize from them and these proceeds may not be adequate to meet any debt service obligations then due. These alternative measures may not be successful and may not permit us to meet our scheduled debt service obligations. If we cannot make scheduled payments on our indebtedness, we will be in default and holders of our Senior Notes could declare all outstanding principal and interest to be due and payable, the lenders under our revolving facility could terminate their commitments to loan money, our secured lenders could foreclose against the assets securing their borrowings and we could be forced into bankruptcy or liquidation. If we breach the covenants under our debt instruments, we would be in default under such instruments. The holders of such indebtedness could exercise their rights, as described above, and we could be forced into bankruptcy or liquidation. Our revolving facility and the indenture that governs our Senior Notes contain terms which restrict our current and future operations, particularly our ability to respond to changes or to take certain actions. Our revolving facility and the indenture that governs our Senior Notes contain a number of restrictive covenants that impose significant operating and financial restrictions on us and may limit our ability to engage in acts that may be in our long- term best interest, including, among other things, restrictions on our ability to: • incur additional indebtedness and guarantee indebtedness; • prepay, redeem or repurchase certain indebtedness; • sell or otherwise dispose of assets; • incur liens; • enter into transactions with affiliates; • alter the businesses we conduct; • enter into agreements restricting our subsidiaries' ability to pay dividends; and • consolidate, merge with, or sell all or substantially all of our assets to, another person. The covenants in the indenture and supplemental indenture that govern the Senior Notes are subject to exceptions and qualifications. In addition, the restrictive covenants in the credit agreement governing our revolving facility require us to maintain specified financial ratios and satisfy other financial condition tests. Our ability to meet those financial ratios and tests can be affected by events beyond our control, and we may not be able to meet them. These restrictive covenants could adversely affect our ability to: • finance our operations; • make needed capital expenditures; • make strategic acquisitions or investments or enter into joint ventures; • withstand a future downturn in our business, the industry or the economy in general; • engage in business activities, including future opportunities, that may be in our best interest; and • plan for or react to market conditions or otherwise execute our business strategies. These restrictions may affect our ability to expand our business, which could have a material adverse effect on our business, financial condition and results of operations. As a result of these restrictions, we will be limited as to how we conduct our business and we may be unable to raise additional debt or equity financing to compete effectively or to take advantage of new business opportunities. The terms of any future indebtedness we may incur could include more restrictive covenants. We cannot assure you that we will be able to maintain compliance with these covenants in the future and, if we fail to do so, that we will be able to obtain waivers from the lenders and / or amend the covenants. Our failure to comply with the restrictive covenants described above and / or the terms of any future indebtedness from time to time could result in an event of default, which, if not cured or waived, could result in our being required to repay these borrowings before their due date. If we are forced to refinance these borrowings on less favorable terms or cannot refinance these borrowings, our business, financial condition and results of operations could be adversely affected. Our revolving facility and the indenture that governs our Senior Notes contain cross- default provisions that could result in the acceleration of all of our indebtedness. A breach of the covenants under our revolving facility or the indenture that governs our Senior Notes could result in an event of default under the applicable indebtedness. Such a default may allow the creditors to accelerate the related indebtedness and may result in the acceleration of any other indebtedness to which a cross- acceleration or cross- default provision applies. In addition, an event of default under the credit agreement governing our revolving facility would permit the lenders under our revolving facility to terminate all commitments to extend further credit under that facility. Furthermore, if we were unable to repay amounts due and payable under our revolving facility, those lenders could proceed against the collateral granted to them to secure that indebtedness. In the event our lenders or noteholders accelerate the repayment of our borrowings, we and our guarantors may not have sufficient assets to repay that indebtedness. Additionally, we may not be able to borrow money from other lenders to enable us to refinance our indebtedness. General Risk Factors If we fail to maintain an effective system of internal controls, 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 Exchange Act, the Sarbanes- Oxley Act of 2002 (" Sarbanes- Oxley Act "), the rules and regulations of Nasdaq, and other securities rules and regulations that impose various requirements on public companies. Our management and other personnel devote substantial time and resources to comply with these rules and regulations. Such compliance has increased, and will continue to increase our legal, accounting and financial compliance costs; make some activities more difficult, time- consuming and costly, and place significant strain on our personnel, systems and resources. The Sarbanes- Oxley Act requires, among other things, that we maintain effective disclosure controls and procedures and internal control over financial reporting. We are continuing to develop and refine our disclosure controls, internal control over financial reporting and other procedures that are designed to ensure information required to be disclosed by us in our consolidated financial statements and in the reports that we file with the SEC is recorded, processed, summarized and reported within the time periods specified in SEC rules and forms, and information required to be disclosed in reports under the Exchange Act is accumulated and communicated to our principal executive and financial officers. Our current controls and any new controls we develop may become inadequate because of changes in conditions in our business. Additionally, to the extent we acquire other businesses, the acquired company may not have a sufficiently robust system of internal controls and we may uncover new deficiencies. Weaknesses in our internal controls may be discovered in the future. Any failure to develop or maintain effective controls, or any difficulties encountered in their implementation or improvement, could harm our results of operations, may result in a restatement of our consolidated financial statements for prior periods, cause us to fail to meet our reporting obligations, and could result in an adverse opinion regarding our internal control over financial reporting from our independent registered public accounting firm, and lead to investigations or sanctions by regulatory authorities. Section 404 of the Sarbanes- Oxley Act requires our management to certify financial and other information in our quarterly and annual reports

and provide an annual management report on the effectiveness of our internal control over financial reporting. We are also required to have our independent registered public accounting firm attest to, and issue an opinion on, the effectiveness of our internal control over financial reporting. If we are unable to assert that our internal control over financial reporting is effective, or if, when required, our independent registered public accounting firm is unable to express an opinion on the effectiveness of our internal control over financial reporting, we could lose investor confidence in the accuracy and completeness of our financial reports, which would cause the price of our Class A common stock to decline. Any failure to maintain effective disclosure controls and internal control over financial reporting could have a material and adverse effect on our business and results of operations and could cause a decline in the price of our stock. Future acquisitions, strategic investments, partnerships, or alliances could be difficult to identify and integrate, divert the attention of key management personnel, disrupt our business, dilute stockholder value and adversely affect our business, financial condition, and results of operations. As part of our business strategy, we have in the past and expect to continue to make investments in and / or acquire complementary companies, services or technologies. Our ability as an organization to acquire and integrate other companies, services or technologies in a successful manner in the future is not guaranteed. We may not be able to find suitable acquisition candidates, and we may not be able to complete such acquisitions on favorable terms, if at all. If we do complete acquisitions, we may not ultimately strengthen our competitive position or ability to achieve our business objectives, and any acquisitions we complete could be viewed negatively by our end- customers or investors. In addition, our due diligence may fail to identify all of the problems, liabilities or other shortcomings or challenges of an acquired business, product or technology, including issues related to intellectual property, product quality or product architecture, regulatory compliance practices, revenue recognition or other accounting practices or issues with employees or customers. If we are unsuccessful at integrating such acquisitions, or the technologies associated with such acquisitions, into our company, the revenue and results of operations of the combined company could be adversely affected. Any integration process may require significant time and resources, and we may not be able to manage the process successfully. We may not successfully evaluate or utilize the acquired technology or personnel, or accurately forecast the financial impact of an acquisition transaction, causing unanticipated write- offs or accounting charges. We may have to pay cash, incur debt or issue equity securities to pay for any such acquisition, each of which could adversely affect our financial condition and the market price of our Class A common stock. The sale of equity or issuance of debt to finance any such acquisitions could result in dilution to our stockholders. The incurrence of indebtedness would result in increased fixed obligations and could also include covenants or other restrictions that would impede our ability to manage our operations. Additional risks we may face in connection with acquisitions include: • diversion of management time and focus from operating our business to addressing acquisition integration challenges; • coordination of research and development and sales and marketing functions; • integration of administrative systems, employee, product and service offerings; • retention of key employees from the acquired company; • changes in relationships with strategic partners as a result of product acquisitions or strategic positioning resulting from the acquisition; • the need to implement or improve controls, procedures, and policies at a business that prior to the acquisition may have lacked sufficiently effective controls, procedures and policies; • additional legal, regulatory or compliance requirements; • financial reporting, revenue recognition or other financial or control deficiencies of the acquired company that we do not adequately address and that cause our reported results to be incorrect; • liability for activities of the acquired company before the acquisition, including intellectual property infringement claims, violations of laws, commercial disputes, tax liabilities and other known and unknown liabilities; and • litigation or other claims in connection with the acquired company, including claims from terminated employees, customers, former stockholders or other third parties. Our failure to address these risks or other problems encountered in connection with acquisitions and investments could cause us to fail to realize the anticipated benefits of these acquisitions or investments, cause us to incur unanticipated liabilities, and harm our business generally. Our corporate structure and intercompany arrangements are subject to the tax laws of various jurisdictions, and we could be obligated to pay additional taxes, which would harm our results of operations. We are expanding our international operations and staff to support our business in international markets. We generally conduct our international operations through wholly- owned subsidiaries and are or may be required to report our taxable income in various jurisdictions worldwide based upon our business operations in those jurisdictions. Our intercompany relationships are subject to complex transfer pricing regulations administered by taxing authorities in various jurisdictions. The amount of taxes we pay in different jurisdictions may depend on the application of the tax laws of the various jurisdictions, including the United States, to our international business activities, changes in tax rates, new or revised tax laws or interpretations of existing tax laws and policies, and our ability to operate our business in a manner consistent with our corporate structure and intercompany arrangements. The relevant taxing authorities may disagree with our determinations as to the income and expenses attributable to specific jurisdictions. If such a disagreement were to occur, and our position was not sustained, we could be required to pay additional taxes, interest and penalties, which could result in one- time tax charges, higher effective tax rates, reduced cash flows and lower overall profitability of our operations. We are subject to federal, state, and local income, sales, and other taxes in the United States and income, withholding, transaction, and other taxes in numerous foreign jurisdictions. Significant judgment is required in evaluating our tax positions and our worldwide provision for taxes. During the ordinary course of business, there are many activities and transactions for which the ultimate tax determination may be uncertain. In addition, our tax obligations and effective tax rates could be adversely affected, among other things, by (i) changes in the relevant tax, accounting and other laws, regulations, principles and interpretations, including increases in corporate tax rates and greater taxation of international income and changes relating to income tax nexus, (ii) recognizing tax losses or lower than anticipated earnings in jurisdictions where we have lower statutory rates and higher than anticipated earnings in jurisdictions where we have higher statutory rates, (iii) changes in foreign currency exchange rates, or (iv) changes in the valuation of our deferred tax assets and liabilities. We may be audited in various jurisdictions, and such jurisdictions may assess additional taxes, sales taxes and value added taxes against us. Although we believe our tax estimates are reasonable, the final determination of any tax audits or litigation could be materially

different from our historical tax provisions and accruals, which could have an adverse effect on our results of operations or cash flows in the period or periods for which a determination is made. In addition, the Organization for Economic Cooperation and Development (" OECD ") has published proposals covering a number of issues, including country- by- country reporting, permanent establishment rules, transfer pricing rules, tax treaties , and taxation of the digital economy. ~~A significant majority of countries in~~ **On October 8, 2021,** the OECD ~~' s~~ **/ G20 inclusive framework on Base Erosion and Profit Shifting (the "** Inclusive Framework **") published** ~~have agreed in principle to~~ a ~~proposed solution to address~~ **statement updating and finalizing** the **key components** ~~tax challenges arising from the digitalization~~ of ~~the economy, including joining~~ a two- pillar plan ~~to~~ **on global tax** reform ~~international taxation rules~~ **originally agreed on July 1, 2021,** and ~~ensure that~~ **a timetable for implementation by 2023. The timetable for implementation has since been extended to 2024 and, with respect to certain components of the plan, to 2025. Under pillar one, a portion of the residual profits of** multinational **businesses** ~~enterprises pay a fair share of tax wherever they operate. The first pillar is focused on the allocation of taxing rights between countries for in- scope multinational enterprises that sell goods and services into countries with little or no local physical presence and is intended to apply to multinational enterprises~~ with global ~~revenue~~ **turnover** above **€** 20 billion ~~euro~~ and ~~certain other criteria~~ **a profit margin above 10 % will be allocated to market jurisdictions where such allocated profits would be taxed** . **Under** ~~The second~~ pillar ~~is focused~~ **two, the Inclusive Framework has agreed** on ~~developing~~ a global minimum **corporate** tax rate of ~~at least~~ 15 **% for companies** ~~percent applicable to in- scope multinational enterprises and is intended to apply to multinational enterprises~~ with ~~annual consolidated group~~ revenue **above €** ~~in excess of~~ 750 million ~~euro~~ **, calculated on a jurisdictional basis** . While substantial work remains to be completed by the OECD and national governments on the implementation of these proposals, future tax reform resulting from these developments may result in changes to long- standing tax principles, which could adversely affect our effective tax rate or result in higher cash tax liabilities. ~~The~~ **On February 1, 2023, the U. S. Financial Accounting Standards Board (" FASB") indicated that they believe the minimum tax imposed under pillar two is an alternative minimum tax, and, accordingly, deferred tax assets and liabilities associated with the minimum tax would not be recognized or adjusted for the estimated future effects of the minimum tax but would be recognized in the period incurred. In addition, the** OECD' s proposed solution envisages new international tax rules and the removal of all Digital Services Taxes (" DST "). Notwithstanding this, some countries, in the European Union and beyond, continue to operate ~~a~~ **existing** DST ~~regime~~ **regimes** to capture tax revenue on digital services more immediately. Such laws may increase our tax obligations in those countries or change the manner in which we operate our business. Our ability to use our net operating loss carryforwards and certain other tax attributes may be limited. As of January 31, ~~2023~~ **2024** , we had aggregate U. S. federal and California net operating loss carryforwards of $ 1. ~~6~~ **5** billion and $ ~~248~~ **243** . ~~2~~ **9** million, respectively, which may be available to offset future taxable income for income tax purposes. **The** ~~If not utilized, the~~ federal **net operating losses are carried forward indefinitely,** and California net operating loss carryforwards will begin to expire in ~~fiscal 2031~~ **2032** . As of January 31, ~~2023~~ **2024** , we had net operating loss carryforwards for other states of $ ~~1.~~ 0 **. 8** billion that will begin to expire in fiscal ~~2024~~ **2025** . As of January 31, ~~2023~~ **2024** , we had federal and California research and development credit carryforwards of $ ~~87~~ **113. 9 million and $ 27** . 4 ~~million and $ 18. 8~~ million, respectively. The federal research and development credit carryforwards will begin to expire in ~~2035~~ **2036** , and the California carryforwards are carried forward indefinitely. As of January 31, ~~2023~~ **2024** , we had aggregate United Kingdom net operating loss carryforwards of $ ~~80~~ **78** . ~~9~~ **0 million and Israel net operating loss carryforwards of $ 51. 5** million, which are carried forward indefinitely. Realization of these net operating loss and research and development credit carryforwards depends on future income, and there is a risk that our existing carryforwards could expire unused and be unavailable to offset future income tax liabilities, which could adversely affect our results of operations. In addition, under Sections 382 and 383 of the Internal Revenue Code, if a corporation undergoes an " ownership change, " generally defined as a greater than 50 % change (by value) in ownership by " 5 percent shareholders " over a rolling three- year period, the corporation' s ability to use its pre- change net operating loss carryovers and other pre- change tax attributes, such as research and development credits, to offset its post- change income or taxes may be limited. We may experience ownership changes in the future as a result of shifts in our stock ownership. As a result, if we earn net taxable income, our ability to use our pre- change net operating loss carryforwards to offset U. S. federal taxable income may be subject to limitations, which could potentially result in increased future tax liability to us. Taxing authorities may successfully assert that we should have collected or in the future should collect sales and use, value added or similar taxes, and we could be subject to liability with respect to past or future sales, which could adversely affect our results of operations. We do not collect sales and use, value added or similar taxes in all jurisdictions in which we have sales because we have been advised that such taxes are not applicable to our services in certain jurisdictions. Sales and use, value added, and similar tax laws and rates vary greatly by jurisdiction. Certain jurisdictions in which we do not collect such taxes may assert that such taxes are applicable, which could result in tax assessments, penalties and interest, to us or our customers for the past amounts, and we may be required to collect such taxes in the future. If we are unsuccessful in collecting such taxes from our customers, we could be held liable for such costs, which may adversely affect our results of operations. If our estimates 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 U. S. GAAP requires management to make estimates and assumptions that affect the amounts reported in our consolidated financial statements and accompanying notes. We base our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, as discussed in the section titled " Management' s Discussion and Analysis of Financial Condition and Results of Operations. " The results of these estimates form the basis for making judgments about the carrying values of assets, liabilities and equity, and the amount of revenue and expenses that are not readily apparent from other sources. Significant assumptions and estimates used in preparing our consolidated financial statements include those related to revenue recognition; allowance for credit losses; valuation of common stock and redeemable convertible preferred stock warrants; carrying value and useful lives of

long- lived assets; loss contingencies; and the provision for income taxes and related deferred taxes. ~~Additionally, as a result of the global COVID- 19 pandemic, many of management' s estimates and assumptions require increased judgment and carry a higher degree of variability and volatility.~~ 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 market price of our Class A common stock. Additionally, we regularly monitor our compliance with applicable financial reporting standards and review new pronouncements and drafts thereof that are relevant to us. As a result of new standards, changes to existing standards and changes in their interpretation, we might be required to change our accounting policies, alter our operational policies and implement new or enhance existing systems so that they reflect new or amended financial reporting standards, or we may be required to restate our published financial statements. Such changes to existing standards or changes in their interpretation may have an adverse effect on our reputation, business, financial position and profit, or cause an adverse deviation from our revenue and operating profit target, which may negatively impact our financial results. We are subject to risks associated with our equity investments, including partial or complete loss of invested capital, and significant changes in the fair value of this portfolio could adversely impact our financial results. Through our Falcon Funds, we invest in early to late stage private companies, and we may not realize a return on our equity investments. Many such companies generate net losses and the market for their products, services, or technologies may be slow to develop or never materialize. These companies are often dependent on the availability of later rounds of financing from banks or investors on favorable terms to continue their operations. The financial success of our investment in any company is typically dependent on a liquidity event, such as a public offering, acquisition, or other favorable market event reflecting appreciation to the cost of our initial investment. The capital markets for public offerings and acquisitions are dynamic and the likelihood of liquidity events for the companies in which we have invested could deteriorate, which could result in a loss of all or a substantial part of our investment in these companies. In addition, our ability to realize gains on investments may be impacted by our contractual obligations to hold securities for a set period of time. For example, to the extent a company we have invested in undergoes an initial public offering, we may be subject to a lock- up agreement that restricts our ability to sell our securities for a period of time after the public offering or otherwise impedes our ability to mitigate market volatility in such securities. Further, valuations of non- marketable equity investments are inherently complex due to the lack of readily available market data. In addition, we may experience additional volatility to our statements of operations due to changes in market prices of our marketable equity investments, the valuation and timing of observable price changes or impairments of our non- marketable equity investments, and changes in the proportionate share of earnings and losses or impairment of our equity investments accounted for under the equity method. This volatility could be material to our results in any given quarter and may cause our stock price to decline. **Expectations of our performance relating to environmental, social and governance factors may impose additional costs and expose us to new risks. There is an increasing focus from regulators, certain investors, and other stakeholders concerning environmental, social and governance (" ESG ") matters, both in the United States and internationally. We have undertaken and expect to continue to undertake certain ESG- related initiatives, goals and commitments, which we have communicated on our website, in our SEC filings and elsewhere. These initiatives, goals, or commitments could be difficult to achieve and costly to implement. We could fail to achieve, or be perceived to fail to achieve, our ESG- related initiatives, goals, or commitments. In addition, we could be criticized for the timing, scope or nature of these initiatives, goals, or commitments, or for any revisions to them. Stakeholders could also challenge the accuracy, adequacy, or completeness of our ESG- related disclosures. Our actual or perceived failure to achieve some or all of our ESG- related initiatives, goals, or commitments or maintain ESG practices that meet evolving stakeholder expectations or regulatory requirements could harm our reputation, adversely impact our ability to attract and retain employees or customers and expose us to increased scrutiny from ESG- focused investors, regulatory authorities and others, or subject us to liability. Damage to our reputation or reduced demand for our products may adversely impact our business, financial condition, or results of operations.** Our business is subject to the risks of ~~earthquakes, fire, floods, outbreak of diseases and other natural~~ catastrophic events, ~~and~~ **including, but not limited** to ~~interruption by~~ **, natural events such as earthquakes, fire, floods, and the outbreak of diseases, as well as** man- made problems such as power disruptions, computer viruses ~~,~~ **or** data security breaches ~~or terrorism~~ . Our principal executive offices are located in Austin, Texas, and we also maintain other office locations around the world, including in California and India, that are prone to natural disasters including severe weather and seismic activity. A significant natural disaster, such as an earthquake, a fire, a flood, or significant power outage and other catastrophic events, including the occurrence of a contagious disease or illness, such as COVID- 19, could have a material adverse impact on our business, results of operations, and financial condition. Natural disasters and other catastrophic events such as ~~COVID- 19~~ **public health crises** , could affect our personnel, recovery of our assets, data centers, supply chain, manufacturing vendors, or logistics providers' ability to provide materials and perform services such as manufacturing products or assisting with shipments on a timely basis. In addition, climate change could result in an increase in the frequency or severity of natural disasters. **If** ~~In the event that~~ our or our service providers' information technology systems or manufacturing or logistics abilities are hindered by any of the events discussed above, shipments could be delayed, resulting in missed financial targets, such as revenue and shipment targets, for a particular quarter. In addition, computer malware, viruses and computer hacking, fraudulent use attempts, and phishing attacks have become more prevalent in our industry **and may be further enhanced in frequency or effectiveness through threat actors' use of AI** , and our internal systems may be victimized by such attacks. Although we maintain incident management and disaster response plans, in the event of a major disruption caused by a **catastrophic event, such as a** natural disaster **,** or man- made problem, we may be unable to continue our operations and may endure system interruptions, reputational harm, delays in our development activities, lengthy interruptions in service, breaches of data security and loss of critical data, and our insurance may not cover such events or may be insufficient to compensate us for the potentially significant losses we may incur ~~. Acts of~~

~~terrorism and other geopolitical unrest could also cause disruptions in our business or the business of our supply chain, manufacturers, logistics providers, partners, or customers or the economy as a whole. Any disruption in the business of our supply chain, manufacturers, logistics providers, partners or end- customers could have a significant adverse impact on our financial results~~ . All of the aforementioned risks may be further increased if the disaster recovery plans for us and our suppliers prove to be inadequate. To the extent that any of the above should result in delays or cancellations of customer orders, ~~or the delay~~ **delays** in the manufacture, deployment or shipment of our products **, or delays in the rendering of our services** , our business, financial condition and results of operations would be adversely affected.