Risk Factors Comparison 2025-03-21 to 2024-03-29 Form: 10-K

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

Our operations and financial results are subject to various risks and uncertainties, including those described below. You should consider and read carefully all of the risks and uncertainties described below, together with all of the other information contained in this Form 10- K, including the section titled " Management' s Discussion and Analysis of Financial Condition and Results of Operations " and our consolidated financial statements and the related notes. The occurrence of any of the following risks or additional risks and uncertainties not presently known to us or that we currently believe to be immaterial could materially and adversely affect our business, financial condition or results of operations. In such case, the trading price of our Class A common stock could decline and stockholders may lose all or part of their investment. Summary of Selected Risk Factors Associated with Our Business The following is only a summary of the principal risks associated with an investment in our Class A common stock. Material risks that may adversely affect our business, financial condition or results of operations include, but are not limited to, the following: • Our recent ~~rapid~~ growth may not be indicative of our future growth. Our ~~rapid~~ growth also makes it difficult to evaluate our future prospects and may increase the risk that we will not be successful. • We have incurred significant net losses in ~~recent years, we may incur losses in~~ the ~~future~~ **past** and we may not be able to generate sufficient revenue to achieve and maintain profitability. • If we fail to effectively manage our growth and organizational change, our business and results of operations could be harmed **. • If we are not able to effectively develop platform enhancements, introduce new products or keep pace with technological developments, our business, results of operations and financial condition could be adversely affected** . • Our actual operating results may differ significantly from any guidance provided. • Our results of operations and financial metrics may be difficult to predict. As a result, we may fail to meet or exceed the expectations of investors or securities analysts, which could cause our stock price to decline. • Any failure of our Unified Customer Experience Management (" Unified- CXM ") platform to satisfy customer demands, achieve increased market acceptance or adapt to changing market dynamics would adversely affect our business, results of operations, financial condition and growth prospects. • The market for Unified- CXM solutions is ~~new and~~ rapidly evolving, and if this market develops more slowly than we expect or declines, develops in a way that we do not expect, or if we do not compete effectively, our business could be adversely affected. • Our business depends on our customers renewing their subscriptions and on us expanding our sales to existing customers. Any decline in our customer renewals or expansion would harm our business, results of operations and financial condition. • We use artificial intelligence in our products, which may result in operational challenges, legal liability, reputational concerns and competitive risks. • Our business and growth depend in part on the success of our strategic relationships with third parties, as well as on the continued availability and quality of feedback data from third parties over whom we do not have control. • Any failure to obtain, maintain, protect, defend or enforce our intellectual property rights could impair our ability to protect our proprietary technology and our brand and adversely affect our business, financial condition and results of operations. • We **and the third parties with whom we work** are subject to stringent and changing obligations related to data privacy and security. Our **(or the third parties with whom we work)** actual or perceived failure to comply with such obligations could lead to regulatory investigations or actions, litigation or mass arbitration demands, fines and penalties, disruptions of our business operations, reputational harm, loss of revenue or profits, loss of customers or sales, and other adverse business consequences. • If we or the third parties ~~upon which~~ **with whom** we ~~rely~~ **work** experience a cybersecurity breach or other security incident **, any vulnerabilities are identified,** or unauthorized parties otherwise obtain access to our customers' data, our data or our Unified- CXM platform, our Unified- CXM platform may be perceived as not being secure, our reputation may be harmed, demand for our Unified- CXM platform may be reduced and we may incur significant liabilities. • Our stock price may be volatile, and the value of our Class A common stock may decline. • Our directors, executive officers and their respective affiliates are able to exert significant control over us, which limits your ability to influence the outcome of important transactions, including a change of control. • Unstable market and economic conditions and catastrophic events may have serious adverse consequences on our business, financial condition and share price. Risks Related to Our Growth Our revenue was $ ~~732~~ **796** . 4 million, $ **732. 4 million, and $** 618. 2 million ~~, and $ 492. 4 million~~ for ~~the each of~~ the years ended January 31, **2025,** 2024, **and** 2023 ~~, and 2022~~ , respectively. You should not rely on the revenue growth of any prior quarterly or annual period as an indication of our future performance. Even if our revenue continues to increase, our revenue growth rate may decline in the future as a result of a variety of factors, including the maturation of our business. Overall growth of our revenue depends on a number of factors, including our ability to: • price our products effectively so that we are able to attract new customers and expand sales to our existing customers; • expand the functionality and use cases for the products we offer on our Unified- CXM platform; • provide our customers with **effective and efficient implementations, as well as on- going** support that meets their needs; • continue to introduce our products to new markets outside of the United States; • successfully identify and acquire or invest in businesses, products or technologies that we believe could complement or expand our Unified- CXM platform; and • increase awareness of our brand on a global basis and successfully compete with other companies. We may not successfully accomplish any of these objectives, and, as a result, it is difficult for us to forecast our future results of operations. If the assumptions that we use to plan our business are incorrect or change in reaction to changes in the markets in which we operate, or if we are unable to maintain consistent revenue or revenue growth, our stock price could be volatile, and it may be difficult to achieve and maintain profitability. You should not rely on our revenue for any prior quarterly or annual periods as an indication of our future revenue or revenue growth. We have incurred significant net losses in ~~recent years, including a net loss of $ 55. 7 million and $ 111. 5 million for~~ the **past** ~~years ended January 31~~ , ~~2023~~ and **we** ~~2022, respectively. We~~ had an

accumulated deficit of $ **626. 1 million and $** 474. 8 million ~~and $ 496. 6 million~~ as of January 31, **2025 and** 2024 ~~and 2023~~, respectively **. While we have experienced revenue growth in recent periods and periods of profitability, we are not certain whether or when we will obtain a high enough volume of sales to sustain or increase our growth or maintain profitability in the future** . We expect that our costs will increase over time and ~~our~~ **we could incur future** losses ~~may continue~~, as we expect to invest significant additional funds in our business ~~and incur costs relating to operating as a public company~~. To date, we have financed our operations principally through subscription payments by customers for use of our Unified- CXM platform and equity and debt financings. We have expended and expect to continue to expend substantial financial and other resources on: • our Unified- CXM platform, including investing in our research and development team, developing or acquiring new products, features and functionality and improving the scalability, availability and security of our Unified- CXM platform; • our technology infrastructure, including expansion of our activities with public cloud service providers, enhancements to our network operations and infrastructure design, and hiring of additional employees for our operations team; • sales and marketing, including expansion of our direct sales organization and marketing efforts; and • additional international expansion in an effort to increase our customer base and sales. These investments may be more costly than we expect and may not result in increased revenue or growth in our business. Any failure to increase our revenue sufficiently to keep pace with our investments and other expenses could prevent us from ~~achieving and~~ maintaining profitability or positive cash flow on a consistent basis. If we are unable to successfully address these risks and challenges as we encounter them, our business, results of operations and financial condition would be adversely affected. In the event that we fail to ~~achieve or~~ maintain profitability, the value of our Class A common stock could decline. We have experienced, and may continue to experience, ~~rapid~~ growth and organizational change, which has placed, and may continue to place, significant demands on our management, operational and financial resources. In addition, we operate globally and sell subscriptions in more than 80 countries **. We also have experienced significant growth in the number of enterprises, end users, transactions and amount of data that our Unified- CXM platform and our associated hosting infrastructure support. As we continue to enter new markets and expand our international operations, we have launched new product innovations in recent years, which has led, and could continue to lead, to increased product and operational complexity, including increased implementation periods, or more complex implementations and ongoing support needs, which could adversely affect our business, results of operations and financial condition** . We plan to continue to expand our international operations into other countries in the future, which will place additional demands on our resources and operations ~~. We also have experienced significant growth in the number of enterprises, end users, transactions and amount of data that our Unified- CXM platform and our associated hosting infrastructure support~~. In order to grow our business, we must continue to attract new customers in a cost- effective manner and enable such customers to realize the benefits associated with our Unified- CXM platform. We may not be able to attract new customers to our Unified- CXM platform for a variety of reasons, including as a result of their use of traditional approaches to customer experience management, their internal timing or budget or the pricing of our Unified- CXM platform compared to products and services offered by our competitors. After a customer makes a purchasing decision, we often must also help them successfully implement our Unified- CXM platform in their organization ~~, a process that can last several months~~. In addition, we have expanded and may attempt to further grow our business by selling our Unified- CXM platform to U. S. federal, state, and local, as well as foreign, governmental agency customers. Growing our business by increasing the number of governmental agency customers we service would subject us to a number of challenges and risks. Selling to such agencies can be highly competitive and time- consuming, often requiring significant upfront time and expenses without any assurance that these efforts will generate a sale. We may not satisfy certain government contracting requirements necessary to attain certification to sell our Unified- CXM platform to certain governmental agency customers. Such government contracting requirements may change and in doing so restrict our ability to sell into the government sector until we have attained the revised certification. Government demand and payment for our products are affected by public sector budgetary cycles and funding authorizations, with funding reductions or delays adversely affecting public sector demand for our products and services. Finally, sales of our Unified- CXM platform to governmental agency customers that are engaged in certain sensitive industries, including organizations whose products or activities are perceived to be harmful, could result in public criticism and reputational risks, which could engender dissatisfaction among potential customers, investors and employees with how we address political and social concerns in our business activities. If we are unable to grow our business by increasing the number of governmental agency customers we service, or if we fail to overcome the challenges and risks associated with selling to such entities, our business, results of operations and financial condition may be adversely affected. Risks Related to Our Business and Industry Our guidance, including forward- looking statements, is prepared by management and is qualified by, and subject to, a number of assumptions and estimates that, while presented with numerical specificity, are inherently subject to significant business, economic and competitive uncertainties and contingencies. Many of these uncertainties and contingencies are beyond our control and are based upon specific assumptions with respect to future business decisions, some of which will change. We generally state possible outcomes as high and low ranges, which are intended to provide a sensitivity analysis as variables are changed but are not intended to represent that actual results could not fall outside of the suggested ranges. Guidance is necessarily speculative in nature, and it can be expected that some or all of the assumptions of the guidance furnished by us will not materialize or will vary significantly from actual results. In particular, guidance offered in periods of extreme uncertainty, such as the uncertainty caused by macroeconomic conditions, is inherently more speculative in nature than guidance offered in periods of relative stability. **For example, we recorded a higher than expected provision for credit losses in the second quarter of fiscal year 2025, which caused certain of our operating results to fall below the guidance ranges provided for such metrics in the previous period.** Accordingly, any guidance with respect to our projected financial performance is necessarily only an estimate of what management believes is realizable as of the date the guidance is given. Actual results will vary from the guidance **,** and the variations may be material. Investors should also recognize that the reliability of any forecasted

financial data will diminish the farther in the future that the data is forecasted. Actual operating results may be different from our guidance, and such differences may be adverse and material. In light of the foregoing, investors are urged to put the guidance in context and not to place undue reliance on it. In addition, the market price of our Class A common stock may reflect various market assumptions as to the accuracy of our guidance. If our actual results of operations fall below the expectations of investors or securities analysts, the price of our Class A common stock could decline substantially. Our results of operations and financial metrics, including the levels of our revenue, gross margin, profitability, cash flow and deferred revenue, have fluctuated in the past and may vary significantly in the future. As a result, period- to- period comparisons of our results of operations may not be meaningful, and the results of any one period should not be relied upon as an indication of future performance. Our results of operations may fluctuate as a result of a variety of factors, many of which are outside of our control, and, as a result, may not fully reflect the underlying performance of our business. Fluctuation in results of operations may negatively impact the value of our Class A common stock. Factors that may cause fluctuations in our results of operations include, without limitation, those listed below: • ~~variability in our sales cycle, including as a result of the budgeting cycles and internal purchasing priorities of our customers; •~~ the payment terms and subscription term length associated with sales of our Unified- CXM platform and their effect on our bookings and free cash flow; • **our ability to successfully implement the software systems we sell; • the timing and success of introductions of new platform features and services by us or our competitors or any other change in the competitive dynamics of our industry, including consolidation among competitors, customers or strategic partners; • increases or decreases in the number of elements of our services or pricing changes upon any renewals of customer agreements; • variability in our sales cycle, including as a result of the budgeting cycles and internal purchasing priorities of our customers; • pricing adjustments made to existing customer agreements; •** the addition or loss of large customers, including through acquisitions or consolidations ~~; • the timing of sales and recognition of revenue, which may vary as a result of changes in accounting rules and interpretations; • the amount and timing of operating expenses related to the maintenance and expansion of our business, operations and infrastructure; • network outages or actual or perceived security breaches or other incidents; • general economic, market and political conditions~~ ; • customer renewal rates; • ~~increases or decreases in the number of elements of our services or pricing changes upon any renewals of customer agreements; •~~ changes in our pricing policies or those of our competitors; • the mix of services sold during a period; • the **amount and timing of operating expenses related to the maintenance and expansion of our business, operations and infrastructure; • our ability to collect on accounts receivable; • the** timing of our recognition of stock- based compensation expense for our equity awards, particularly in cases where awards covering a large number of our shares are tied to a specific event or date; ~~and~~ • the timing ~~and success~~ of **sales** ~~introductions of new platform features~~ and ~~services by us or~~ **recognition of revenue, which may vary as a result of changes in accounting rules and interpretations; • network outages** ~~our~~ **or** ~~competitors~~ **actual** or ~~any~~ **perceived security breaches or** other **incidents; and • general economic** ~~change in the competitive dynamics of our industry~~ , **market and political conditions** ~~including consolidation among competitors, customers or strategic partners~~ . The cumulative effects of the factors discussed above could result in large fluctuations and unpredictability in our quarterly and annual results of operations. This variability and unpredictability also could result in our failing to meet the expectations of industry or financial analysts or investors for any period. If our revenue or results of operations fall below the expectations of analysts or investors or below any guidance we may provide, or if the guidance we provide is below the expectations of analysts or investors, the price of our Class A common stock could decline substantially. Such a stock price decline could occur even if we have met any previously publicly stated guidance we may provide. Any failure of our Unified- CXM platform to satisfy customer demands, achieve increased market acceptance or adapt to changing market dynamics would adversely affect our business, results of operations, financial condition and growth prospects. We derive, have derived and expect to continue to derive the substantial majority of our revenue from subscriptions to our Unified- CXM platform. As such, the market acceptance of our Unified- CXM platform is critical to our success. Demand for our Unified- CXM platform is affected by a number of factors, many of which are beyond our control, including the extension of our Unified- CXM platform for new use cases, the timing of development and release of new products, features and functionality introduced by us or our competitors, technological change and the growth or contraction of the market in which we compete. In addition, we expect that an increasing focus on customer satisfaction and the growth of various communications channels and new technologies will profoundly impact the market for Unified- CXM solutions. We believe that enterprises increasingly are looking for flexible solutions that bridge across traditionally separate systems for experience management, marketing automation and customer relationship management. **We may be unable to effectively adapt our platform and approach to respond to changes in technology and customer needs. For example, in recent periods, we have experienced difficulties with managing the implementation of certain larger CCaaS projects, which has resulted in increased customer dissatisfaction and loss of certain customers.** If we are unable to meet this demand to manage customer experiences through flexible solutions designed to address a broad range of needs, or if we otherwise fail to achieve more widespread market acceptance of our Unified- CXM platform, our business, results of operations, financial condition and growth prospects may be adversely affected. We believe that our success and growth will depend to a substantial extent on the widespread acceptance and adoption of Unified- CXM solutions in general, and of our Unified- CXM platform in particular. The market for Unified- CXM solutions is ~~new and~~ rapidly evolving, and if this market fails to grow or grows more slowly than we currently anticipate, demand for our Unified- CXM platform could be adversely affected. The Customer Experience Management (" CXM ") market also is subject to rapidly changing user demand and trends. As a result, it is difficult to predict enterprise adoption rates and demand for our Unified- CXM platform, the future growth rate and size of our market or the impact of competitive solutions. The expansion of the CXM market depends on a number of factors, including awareness of the Unified- CXM category generally, ease of adoption and use, cost, features, performance and overall platform experience, data security and privacy, interoperability and accessibility across devices, systems and platforms and perceived value. If Unified- CXM solutions do not continue to achieve market acceptance,

or if there is a reduction in demand for Unified- CXM solutions for any reason, including a lack of category or use case awareness, technological challenges, weakening economic conditions, data security or privacy concerns, competing technologies and products or decreases in information technology spending, our business, results of operations and financial condition may be adversely affected. The market for Unified- CXM solutions is also highly competitive. Our competitors may be able to respond more quickly and effectively than we can to new or changing opportunities, technologies, standards or enterprise requirements. With the introduction of new technologies, the evolution of our Unified- CXM platform and new market entrants, we expect competition to intensify in the future. Pricing pressures and increased competition generally could result in reduced sales, reduced margins, losses or the failure of our Unified- CXM platform to achieve or maintain more widespread market acceptance, any one of which could harm our business. While we do not believe that any of our competitors currently offer a full suite of Unified- CXM solutions that competes across the breadth of our Unified- CXM platform, certain features of our Unified- CXM platform compete in particular segments of the overall Unified- CXM category. Our main competitors include, among others, experience management solutions, including ~~solution~~ **social** media **management and social listening** solutions, home- grown ~~solutions and~~ tools, adjacent Unified- CXM solutions, such as social messaging, **conversational and Agenic AI, CCaaS solutions,** customer service and support solutions, ~~traditional~~ **customer feedback management and Voice of the Customer solutions, content** marketing, **and social** advertising **solutions,** and consulting firms and customer relationship management and enterprise resource planning solutions. Further, other established SaaS providers and other technology companies not currently focused on Unified- CXM may expand their services to compete with us. Some of our competitors may be able to offer products or functionality similar to ours at a more attractive price than we can or do, including by integrating or bundling such products with their other product offerings. Additionally, some potential customers, particularly large organizations, have elected, and may in the future elect, to develop their own internal Unified- CXM solutions. Acquisitions, partnerships and consolidation in our industry may provide our competitors even more resources or may increase the likelihood of our competitors offering bundled or integrated products that we may not be able to effectively compete against. In particular, as we rely on the availability and accuracy of various forms of customer feedback and input data, the acquisition of any such data providers or sources by our competitors could affect our ability to continue accessing such data. Furthermore, we also are subject to the risk of future disruptive technologies. If new technologies emerge that are able to collect and process experience data, or otherwise develop Unified- CXM solutions at lower prices, more efficiently, more conveniently or with functionality and features enterprises prefer to ours, such technologies could adversely impact our ability to compete. If we are not able to compete successfully against our current and future competitors, our business, results of operations and financial condition may be adversely affected. In order for us to maintain or improve our results of operations, it is important that we maintain and expand our relationships with our customers and that our customers renew their subscriptions when the initial subscription term expires or otherwise expand their subscription program with us. Our customers are not obligated to, and may elect not to, renew their subscriptions on the same or similar terms after their existing subscriptions expire. Some of our customers have in the past elected, and may in the future elect, not to renew their agreements with us or otherwise reduce the scope of their subscriptions, and we do not have sufficient operating history with our business model and pricing strategy to accurately predict long- term customer renewal rates. In addition, the growth of our business depends in part on our customers expanding their use of our Unified- CXM platform, which can be difficult to predict. Our customer renewal rates, as well as the rate at which our customers expand their use of our Unified- CXM platform, may decline or fluctuate as a result of a number of factors, including the customers' satisfaction with our Unified- CXM platform, defects or performance issues, our customer and product **implementation and** support, our prices, mergers and acquisitions affecting our customer base, the effects of global economic conditions, the entrance of new or competing technologies and the pricing of such competitive offerings or reductions in the enterprises' spending levels for any reason. If our customers do not renew their subscriptions, renew on less favorable terms or reduce the scope of their subscriptions, our revenue may decline and we may not realize improved results of operations from our customer base, and, as a result, our business and financial condition could be adversely affected. We recognize revenue over the term of our customers' contracts.Consequently,increases or decreases in new sales may not be immediately reflected in our results of operations and may be difficult to discern.We generally recognize subscription revenue from customers ratably over the terms of their contracts and a majority of our revenue is derived from subscriptions that have terms of one to three years.As a result,a portion of the revenue we report in each quarter is derived from the recognition of deferred revenue relating to subscriptions entered into during previous quarters.Consequently,a decline in new or renewed subscriptions in any single quarter may have a small impact on our revenue results for that quarter.However,such a decline will negatively affect our revenue in future quarters.Accordingly,the effect of significant downturns in sales and market acceptance of our Unified- CXM platform and potential changes in our pricing policies or rate of expansion or retention may not be fully reflected in our results of operations until future periods. **We also** ~~For example,the impact of current economic uncertainties~~ may ~~cause customers to request better pricing,which may not~~ be ~~reflected immediately in~~ **unable to reduce** our ~~results of operations~~ **cost structure in line with a significant deterioration in sales** .In addition, ~~customers have in the past and may continue in the future to slow their rate of expansion or reduce their number of licenses.We also may be unable to reduce our cost structure in line with~~ a significant ~~deterioration in sales.In addition,a~~ majority of our costs are expensed as incurred,while revenue is recognized over the term of the agreements with our customers.As a result,increased growth in the number of our customers could continue to result **in our recognition of more costs than revenue in the earlier periods of the terms of our agreements.Our subscription model also makes it difficult for us to rapidly increase our revenue through additional sales in any period,as revenue from new customers must be recognized over the applicable subscription term.We** rely on third- party data centers and cloud computing providers, and any interruption or delay in service from these facilities could impair the delivery of our Unified- CXM platform and harm our business. We currently serve our customers from third- party data centers and cloud computing providers located around the world. Some of these facilities may be located in areas prone to natural disasters and

may experience events such as earthquakes, floods, fires, severe weather events, power loss, computer or telecommunication failures, service outages or losses, and similar events. They also may be subject to break- ins, sabotage, intentional acts of vandalism and similar misconduct or cybersecurity issues, **including attacks enhanced or facilitated by artificial intelligence (" AI ")** human error, terrorism, improper operation, unauthorized entry and data loss **. Our data center operations also rely heavily on the availability of electricity, which also comes from third- party providers. If we or the third- party data center and cloud computing provider facilities that we use to deliver our services were to experience a major power outage or if the cost of electricity were to increase significantly, our operations and financial results could be harmed. If we or our third- party data centers and cloud service provider facilities were to experience a major power outage, we or they would have to rely on back- up generators, which might not work properly or might not provide an adequate supply during a major power outage. Such a power outage could result in a significant disruption of our business** . In the event of significant physical damage to one of these data centers, it may take a significant period of time to achieve full resumption of our services, and our disaster recovery planning may not account for all eventualities. We also may incur significant costs for using alternative equipment or taking other actions in preparation for, or in reaction to, events that damage the data centers **and equipment** that we use. Although we carry business interruption insurance, it may not be sufficient to compensate us for the potentially significant losses, including the potential harm to the future growth of our business that may result from interruptions in our services or products. As we grow and continue to add new third- party data centers and cloud computing providers and expand the capacity of our existing third- party data centers and cloud computing providers, we may move or transfer our data and our customers' data. Despite precautions taken during this process, any unsuccessful data transfers may impair the delivery of our Unified- CXM platform. Any damage to, or failure of, our systems, or those of our third- party data centers or cloud computing providers or the systems of a customer that hosts our software in their private cloud, could result in interruptions on our Unified- CXM platform or damage to, or loss or compromise of, our data and our customers' data, including personal data. Any impairment of our or our customers' data or interruptions in the functioning of our Unified- CXM platform, whether due to damage to, or failure of, third- party data centers, cloud computing providers or the cloud computing providers of our customers or unsuccessful data transfers, may reduce our revenue **, increase our operations costs** , result in significant fines, cause us to issue credits or pay penalties, subject us to claims for indemnification and other claims, litigation or disputes, result in regulatory investigations or other inquiries, cause our customers to terminate their subscriptions and adversely affect our reputation, renewal rates and our ability to attract new customers. Our business will also be harmed if our existing and potential customers believe that our Unified- CXM platform is unreliable or not secure. Further, our leases and other agreements with data centers and cloud computing providers expire at various times, and the owners of our data center facilities and cloud computing providers have no obligation to renew their agreements with us on commercially reasonable terms, or at all **, which exposes us to the potential for significant cost increases** . Additionally, certain of our data center and clouding computing provider agreements may be terminable for convenience by the counterparty. If services are interrupted at any of these facilities or providers, such agreements are terminated, or we are unable to renew these agreements on commercially reasonable terms or at all, or if one of our data center or cloud computing providers is acquired or encounters financial difficulties, including bankruptcy, we may be required to transfer our **data,** servers and other infrastructure to new data centers and cloud computing providers, and we may incur significant costs and possible service interruptions in connection with doing so. In addition, if we do not accurately plan for our data center and cloud computing capacity requirements and we experience significant strains on our data center and cloud computing capacity, we may experience delays and additional expenses in arranging new data center and cloud computing arrangements, and our customers could experience service outages that may subject us to financial liabilities **due to, for example, breach of Service Level Agreements (SLAs) or other commitments** , result in customer losses and dissatisfaction, and materially adversely affect our business, operating results and financial condition ~~. If we are not able to effectively develop platform enhancements, introduce new products or keep pace with technological developments, our business, results of operations and financial condition could be adversely affected~~ . Our future success will depend on our ability to adapt and innovate. To attract new customers and increase revenue from our existing customers, we will need to enhance and improve our existing platform and introduce new products, features and functionality. Enhancements and new products that we develop may not be introduced in a timely or cost- effective manner, may contain errors or defects, and may have interoperability difficulties with our Unified- CXM platform or other products. **Furthermore, while we generally expect that enhancements and improvements to our products will attract new customers, certain of our customer agreements restrict our ability to materially change the features and functionality of our products, including in some cases, prohibiting the use of AI or generative AI in our products, which could result in violations of those customer agreements, or increased operational difficulties and costs due to our need to deploy different version of our products to different customers, i. e., enable or disable certain features, or failure of such customers to renew their agreements (and therefore, loss in revenue from such customers) as a result of our new products, features, and functionality.** We have in the past experienced **, and may in the future experience,** delays in our ~~internally~~ planned release dates of new products, features and functionality, and there can be no assurance that these developments will be released according to schedule. We also have invested, and may continue to invest, in the acquisition of complementary businesses and technologies that we believe will enhance our Unified- CXM platform. ~~However, we may not be able to integrate these acquisitions successfully or achieve the expected benefits of such acquisitions.~~ If we are unable to successfully develop **, release** , acquire or integrate new products, features and functionality, or enhance our existing platform to meet the needs of our existing or potential customers in a timely and effective manner, or if a customer is not satisfied with the quality of work performed by us or with the technical support services rendered, **our customers may delay or withhold payment to us, cancel their agreements with us, elect not to renew, or make service credit claims, warranty claims or other claims against us, and** we could **lose future sales. The occurrence of any of these events could result in diminishing demand for our solutions, a**

reduction of our revenues, an increase in our provision for credit losses or in collection cycles for accounts receivable or could cause us to incur ~~additional costs to address~~ the **risk** ~~situation, and our~~ **or expense** ~~business, results~~ of **litigation** ~~operations and financial condition could be adversely affected~~. Similarly, our customers and users of our Unified- CXM platform are increasingly accessing our Unified- CXM platform or interacting via mobile devices. We are devoting valuable resources to solutions related to mobile usage, but we cannot assure you that these solutions will be successful. If the mobile solutions we have developed for our Unified- CXM platform do not meet the needs of current or prospective customers, or if our solutions are difficult to access **or use**, customers or users may reduce their usage of our Unified- CXM platform or cease using our Unified- CXM platform altogether and our business could suffer. In addition, because our Unified- CXM platform is designed to operate on a variety of networks, applications, systems and devices, we will need to continually modify and enhance our Unified- CXM platform to keep pace with technological advancements in such networks, applications, systems and devices. If we are unable to respond in a timely, user- friendly and cost- effective manner to these rapid technological developments, our Unified- CXM platform may become less marketable and less competitive or obsolete, and our business, results of operations and financial condition may be adversely affected. We use artificial intelligence in our products and operations, which may result in operational challenges, legal liability, reputational concerns and competitive risks. **We use AI tools in our business operations for internal and external uses. Specifically, our employees and personnel may use AI technologies to support their work and our internal business operations, including for example to generate source code used in our products and systems. Output from generative AI may infringe on third- party intellectual property rights without us being aware. Moreover, advanced AI tools, which may produce content indistinguishable from that generated by humans, have a number of benefits, risks, and liabilities, some still unknown. Recent decisions of governmental entities and courts (such as the U. S. Copyright Office, U. S. Patent and Trademark Office, and U. S. Court of Appeals for the Federal Circuit) interpret U. S. copyright and patent law as limited to protecting works and inventions created by human authors and inventors, respectively. We are therefore unlikely to be able to obtain U. S. copyright or patent protection for works or inventions wholly created by a generative AI tool, and our ability to obtain U. S. copyright and patent protection for source code, text, images, inventions, or other materials, which are developed with some use of AI tools, such as generative AI, may be limited, if available at all. Likewise, the availability of intellectual property protections in other countries is similarly unclear. Additionally, our use of third- party generative AI tools to develop source code, text, images, inventions, or other materials may expose us to greater risks than utilizing contracted human developers, as third- party generative AI vendors typically do not provide warranties or indemnities with respect to the output generated by such generative AI tools, and generative AI tools may also provide output that appears correct but is erroneous. Furthermore, some generative AI tools may be offered under terms that do not protect the confidentiality of the prompts or inputs that users submit to such tools and may use prompts or inputs to train shared AI models, potentially resulting in third- party users receiving outputs containing information from prompts or inputs (including confidential, competitive, proprietary, or personal data) that we submitted to the tool. Our use of generative AI tools to generate code may also present additional security risks because the generated source code may contain security vulnerabilities. Additionally, the vendors of these generative AI tools may fail to comply with their contractual obligations to us regarding the confidentiality or security of any data or other inputs provided to such vendor or outputs generated by their generative AI tools. Our sensitive information could be leaked, disclosed, or revealed as a result of or in connection with our employees', personnel' s, or vendors' use of third- party generative AI tools or AI technologies generally.** In addition to the use of **generative AI in our internal operations, including for generation of code, we also use** our own **proprietary** ~~artificial intelligence ("~~ AI ~~")~~ **- based** features within our products, ~~we~~ **and** have ~~also~~ incorporated generative ~~artificial intelligence (" Generative~~ AI ~~") processes and algorithms~~ into our product offerings ~~and internal operations~~ through third- party **vendors** ~~partners integrated with our products and tools~~, which ~~may~~ **has the potential to** result in adverse effects to our financial condition, results or reputation. Generative AI features and services leverage existing and widely available technologies, such as those owned by **Microsoft Azure,** OpenAI or alternative large language model providers. The use of ~~Generative~~ **generative** AI **technology and** processes at scale is relatively new and may lead to challenges, concerns and risks that are significant or that we may not be able to predict, especially if our use of these technologies in our products and services becomes more important to our operations over time. Use of AI or ~~Generative~~ **generative** AI in our products and services may be difficult to deploy successfully due to operational issues inherent to the nature of such technologies, including the development, maintenance and operation of deep learning datasets **. Further**, ~~and~~ **some of** our customers ~~failing~~ **, especially those in highly regulated industries, may be reluctant or unwilling** to adopt **AI** ~~or implement our~~ **or** ~~new~~ **generative AI products. Accordingly, adoption of generative AI features in our products and marketing our** products as ~~intended~~ **AI or generative AI products could reduce or delay customer adoption**. For example, AI and ~~Generative~~ **generative** AI ~~algorithms~~ use machine learning **techniques, including, but not limited to, algorithms, natural language processing** and / or content creation which, depending on the ~~reliability of the~~ model **and the intended use case**, may lead to flawed, biased, unexplained, and inaccurate results **or outputs**, which could lead to customer rejection or skepticism of such products **or even potentially claims against us arising from customer reliance on erroneous output to its detriment**. Emerging ethical issues surround the use of AI ~~or~~ **and** ~~Generative~~ **generative** AI, ~~and~~ **or** if our deployment or ~~use~~ **development** of AI or ~~Generative~~ **generative** AI becomes controversial or is **successfully and adversely** challenged by our current or prospective customers, we may be subject to reputational risk. Any sensitive information (including confidential, competitive, proprietary, or personal data) that ~~we or~~ our customers input into the third- party ~~Generative~~ **generative** AI features in our products **(or that we input into generative AI tools that we use)** could be leaked ~~or~~ **,** disclosed to others **or used for improper purposes**, including if sensitive information is used to train **our own AI or** the third parties' ~~Generative~~ **generative** AI models, in breach of our contractual agreements. ~~Additionally, where~~ **While we have processes and practices designed to ensure that we have** the ~~product ingests~~

necessary rights to use source training data for training our AI, we may not in every instance be able to confirm that all of the information contained in such datasets has been obtained with the necessary permissions for us to use for purposes of our AI. For example, we may use publicly available data to train our AI that contains information that was unlawfully acquired from third parties without our knowledge. While we have some tools that can be leveraged to help us avoid using personal data **to train or fine- tune ~~or~~ our AI, it may be difficult for us to avoid or identify all instances** where **personal data may be in the scope of the training data, even though** it **is not necessarily required. If we were to receive claims from third parties asserting rights against our use of certain datasets used to train our AI, it may be difficult or impossible to disentangle our trained models from the subject matter of the claims. The disclosure and use of personal data in AI technologies is subject to various privacy laws and other privacy obligations. Additionally, where our products ingest personal data or where they ~~makes~~ make** connections using such data, these AI or ~~Generative~~ **generative** AI processes may reveal **or generate** other personal or sensitive **data over which we ~~information generated by the AI or Generative AI solution, or~~** could ~~lead us to be unable~~ **lose control or impair our ability** to fulfill certain data subject requests in compliance with certain privacy laws **or contractual obligations to our customers**, such as requests to delete certain personal data ingested by the product. Further, unauthorized use or misuse of ~~Generative~~ **generative** AI by our employees **, customers** or others, including violation of internal policies or procedures or guidelines **or contractual agreements and terms (including internal and external Acceptable Use policies or other policies and third- party terms)**, may result in disclosure **or misuse** of confidential company and customer data, reputational harm, privacy law violations, legal **and contractual** liability, or regulatory actions, including algorithmic disgorgement. Improper **development, deployment, or onward** use of AI and ~~Generative~~ **generative** AI ~~could~~ **has the potential to** result in biased ~~results~~ **outcomes** and could lead ~~us~~ to ~~make~~ decisions that could ~~bias~~ **harm** certain individuals (or classes of individuals), and adversely impact their rights, employment, and ability to obtain certain pricing, products, services, or benefits. In addition, ~~our~~ use of ~~Generative~~ **generative** AI may also lead to novel and urgent cybersecurity risks (such as if a bad actor " poisons " the ~~Generative~~ **generative** AI with bad inputs or logic), including the misuse of personal or business confidential data, which may adversely affect our operations and reputation. As a result, the integration of ~~Generative~~ **generative** AI into our products and operations may not be successful despite expending significant time and monetary resources to attempt to ~~do so~~ **make it successful**. Our investments in deploying such technologies may be substantial, and they may be more expensive than anticipated. If we fail to deploy ~~Generative~~ **generative** AI as intended, our competitors may incorporate ~~Generative~~ **generative** AI technology into their products or services more successfully than we do, which may impair our ability to effectively compete in the market. **Furthermore, we make numerous statements online and in our marketing materials describing the availability of AI, as well as our use and integration of generative AI in our products. Although we endeavor to be accurate with our public statements and documentation, we may at times fail to do so or be alleged to have failed to do so. Our statements regarding our AI- supported features and use of generative AI can subject us to potential government or legal action if they are found to be deceptive, unfair or misrepresentative of our actual practices. Should any of these statements prove to be untrue or be perceived as untrue, even though circumstances beyond our reasonable control, we may face litigation, disputes, claims, investigations, inquiries or other proceedings that could adversely affect our business, reputation, results of operations and financial condition.** Uncertainty in the legal regulatory regime relating to AI **, as well as variation on AI regulations from jurisdiction to jurisdiction,** may require significant resources to modify and maintain business practices to comply with U. S. and foreign laws, the nature of which cannot be determined at this time as they continue to **rapidly** evolve and solidify. Several jurisdictions around the globe have already proposed or enacted laws or guidelines governing AI. For example, the ~~Biden administration recently issued~~ **EU Artificial Intelligence Act (" EU AI Act ") has come into force ~~an~~ and its provisions are gradually becoming ~~executive~~ effective ~~order~~, which imposes a number of obligations** on **various parties related to the development and use of certain** AI ~~that requires companies developing certain types of AI models to notify the federal government of certain safety test results and other information. As another example, European regulators have proposed an AI regulation that imposes onerous obligations related to the use of AI~~ **related based** systems, and ~~we expect that~~ other jurisdictions ~~will~~ **are beginning to** adopt **or prepare for adoption of** similar laws. ~~Other jurisdictions~~ **These laws** may **be ~~decide to adopt similar or~~** more restrictive ~~legislation that~~ **than the EU AI Act and** may render the use of such technologies challenging **. While we aim to develop and use AI responsibly by attempting to identify and mitigate any issues associated with fairness, bias, transparency, or ethical or legal use of AI, we may be unsuccessful in identifying or resolving such issues. Further, use of our AI systems for unintended or improper use cases by customer users may alter the associated legal obligations upon Sprinklr, without our knowledge. We may not be able to detect, mitigate and remediate such misuse, and limitations of liability in contracts may be inadequate to address legal liability, fines, penalties and other regulatory actions resulting from such misuse**. Additionally, certain privacy laws extend rights to consumers (such as the right to delete certain personal data) and regulate automated decision making, which may be incompatible with ~~our~~ AI **, particularly training ~~features or our use of Generative~~** AI **using personal data**. These obligations may make it harder for us to conduct our business using AI ~~or Generative~~ **, develop innovative** AI ~~, lead to~~ **models and create potential for** regulatory fines or penalties, require us to change our business practices, retrain our AI, prevent or limit our **creation and** use of AI or ~~Generative~~ **generative** AI, or delete or **require us to** disgorge certain algorithms. For example, the US Federal Trade Commission has required other companies to turn over or delete or disgorge valuable insights or trainings generated through the use of AI, or the AI models or algorithms themselves, where they allege the company has violated privacy and consumer protection laws. ~~If~~ **Our use of AI and generative AI technology could result in additional compliance costs, regulatory investigations and actions, and lawsuits if we do not use (or are perceived to not use it) it in accordance with our internal and external policies and governance, or applicable laws and other obligations, including contractual obligations to our customers. However, if** we cannot use AI or ~~Generative~~ **generative** AI, or that use is restricted, our business may be less

efficient, or we may be at a competitive disadvantage. Further, intellectual property ownership and liability for violation of **terms of use,** open **-** source ~~licenses~~ **license obligations** , infringement or misappropriation of intellectual property and violation of privacy or publicity rights are issues arising from the use of AI technologies that legislators are still attempting to establish and with which courts are still grappling. ~~Therefore~~ **In addition** , **access to data from third- party sources, including public sources and data suppliers, may become more restricted in** the ~~use~~ **future, which could negatively impact our development and deployment** of **products, including** AI technologies **, that rely on such data for training or operation. Therefore, the use of AI technologies** in connection with our products or operations may **impact our business model or** result in the inability to establish ownership of intellectual property or exposure to claims relating to the foregoing ~~. Moreover, our employee and personnel use Generative AI technologies to perform their work, and the disclosure and use of personal data, is subject to various privacy laws and other privacy obligations. Our use of this technology could result in additional compliance costs, regulatory investigations and actions, and lawsuits if we do not use (or are perceived to not use it) it in accordance with our internal policies and governance, applicable laws or other obligations. Output from Generative AI systems that we use may infringe on third party intellectual property rights without us being aware. However, if we are unable to use Generative AI, it could make our business less efficient and result in competitive disadvantages. Additionally, sensitive information of the Company or our customers could be leaked, disclosed, or revealed as a result of or in connection with our employees', personnel' s, or vendors' use of Generative AI technologies~~ . We depend on, and anticipate that we will continue to depend on, various third- party relationships in order to sustain and grow our business, including technology companies whose products integrate with ours. Failure of any of these technology companies to maintain, support or secure their technology platforms in general, and our integrations in particular, or errors or defects in their technologies or products, could adversely affect our relationships with our customers, damage our brand and reputation and result in delays or difficulties in our ability to provide our Unified- CXM platform **. For example, we rely on third parties to support certain components of our communication and voice services. Failure of any of these third- party providers to provide their services or to meet contractual service level commitments, or if they materially increase the cost of their services, for any reason, could adversely affect our relationships with our customers, lead to increases in the prices we are charged and therefore potentially the prices our customers pay for our products and services, damage our brand and reputation and result in delays or difficulties in our ability to provide certain services** . We also rely on the availability and accuracy of various forms of client feedback and input data, including data solicited via survey or based on data sources across modern channels, and any changes in the availability or accuracy of such data could adversely impact our business and results of operations and harm our reputation and brand. In some cases, we rely on negotiated agreements with social media networks and other data providers. These negotiated agreements may provide increased access to application programming interfaces (" APIs ") and data that allow us to provide a more comprehensive solution for our customers. These agreements are subject to termination in certain circumstances, and there can be no assurance that we will be able to renew those agreements or that the terms of any such renewal, including pricing and levels of service, will be favorable. We cannot accurately predict the potential impact of the termination of any of our agreements with social media networks and other data providers, including the impact on our access to the related APIs. There can be no assurance that following any such termination we would be able to maintain the current level of functionality of our platform in such circumstances, as a result of more limited access to APIs or otherwise, which could adversely affect our results of operations. In addition, there can be no assurance that we will not be required to enter into new negotiated agreements with data providers in the future to maintain or enhance the level of functionality of our platform, or that the terms and conditions of such agreements, including pricing and levels of service, will not be less favorable, which could adversely affect our results of operations. In particular, X (formerly known as Twitter) provides us with certain data that supports our Unified- CXM platform pursuant to an agreement that expires on ~~February 28~~ **December 31** , ~~2025~~ **2026** . If our agreement with X ~~(formerly known as Twitter)~~ expires, is not renewed on the same or similar terms or at all, or if it is terminated due to the failure or unwillingness of either party to perform its obligations thereunder, we may not be able to provide the same level of Unified- CXM insights to our customers and our business, results of operations and financial condition may be materially and adversely affected **. In addition, we obtain data from data aggregators who, despite their commercial commitments to us, may not have the right to provide that data to us, and so could expose us to claims in the future, from the data sources or data owners** . We invest significantly in research and development, and, to the extent that our research and development investments do not translate into new solutions or material enhancements to our current solutions or we do not use those investments efficiently, our business and results of operations would be harmed. A key element of our strategy is to invest significantly in our research and development efforts to improve and develop new technologies, features and functionality for our Unified- CXM platform. For each of the years ended January 31, **2025 and** 2024 ~~and 2023~~ , our research and development expenses were at least 10 % of our revenue. If we do not spend our research and development budget efficiently or effectively, our business may be harmed and we may not realize the expected benefits of our strategy. Moreover, research and development projects can be technically challenging, time-consuming and expensive. The nature of these research and development cycles may cause us to experience delays between the time we incur expenses associated with research and development and the time we are able to offer compelling platform updates and generate revenue, if any, from such investment. Additionally, anticipated enterprise demand for a solution or solutions we are developing could decrease after the development cycle has commenced, and we would nonetheless be unable to avoid substantial costs associated with the development of any such solutions or solution. If we expend a significant amount of resources on research and development and our efforts do not lead to the successful introduction or improvement of solutions that are competitive in our current or future markets, our business and results of operations would be adversely affected. If we are unable to develop and maintain successful relationships with channel partners, our business, results of operations, and financial condition could be adversely affected. To date, we primarily have relied on our direct sales force, online marketing and word- of- mouth to sell subscriptions to our Unified- CXM platform. Although we have developed relationships with certain

channel partners, such as referral partners, resellers and integration partners, these channels have resulted in limited revenue to date. We believe that continued growth in our business is dependent upon identifying, developing and maintaining strategic relationships with additional channel partners that can drive additional revenue. Our agreements with our existing channel partners are non- exclusive, meaning our channel partners may offer enterprises the products of several different companies, including products that compete with ours. They also may cease marketing our Unified- CXM platform with limited notice and with little or no penalty. We expect that any additional channel partners we identify and develop will be similarly non- exclusive and not bound by any requirement to continue to market our Unified- CXM platform. If we fail to identify additional channel partners in a timely and cost- effective manner, or at all, if we are unable to assist our current and future channel partners in independently selling and implementing our Unified- CXM platform, or if our channel partners choose to use greater efforts to market their own products or those of our competitors, our business, results of operations and financial condition could be adversely affected. Furthermore, if our channel partners do not effectively market and sell our Unified- CXM platform, or fail to meet the needs of our customers, our reputation and ability to grow our business also may be adversely affected. Sales by channel partners are more likely than direct sales to involve collection issues, in particular sales by our channel partners into developing markets, and, accordingly, variations in the mix between revenue attributable to sales by channel partners and revenue attributable to direct sales may result in fluctuations in our results of operations. If we are not able to maintain and enhance our brand, our business, results of operations and financial condition may be adversely affected. We believe that maintaining and enhancing our reputation as a differentiated and category- defining company in Unified- CXM is critical to our relationships with our existing customers and key employees and to our ability to attract new customers and talented personnel. The successful promotion of our brand depends on a number of factors, including the effectiveness of our marketing efforts, our ability to continue to develop a high- quality platform, our ability to provide reliable services that continue to meet the needs of our customers, our ability to maintain our customers' trust and our ability to successfully differentiate our Unified- CXM platform from competitive solutions, which we may not be able to do effectively. We do not have sufficient operating history to know whether our brand promotion activities will ultimately be successful or yield increased revenue, and, if they are not successful, our business may be adversely affected. Any unfavorable publicity of our business or platform generally, for example, relating to our privacy practices, terms of service, service quality, litigation, regulatory activity, the actions of our employees, partners or customers or the actions of other companies that provide similar solutions to us, all of which can be difficult to predict, could adversely affect our reputation and brand. In addition, independent industry analysts often provide reviews of our Unified- CXM platform, as well as solutions offered by our competitors, and our brand and perception of our Unified- CXM platform in the marketplace may be significantly influenced by these reviews. If these reviews are negative, or less positive compared to those of our competitors' solutions, our brand and market position may be adversely affected. It also may be difficult to maintain and enhance our brand as we expand our marketing and sales efforts through channel or strategic partners. The promotion of our brand also requires us to make substantial expenditures. We anticipate that these expenditures will increase as our market becomes more competitive, as we expand into new markets and as more sales are generated through our channel partners. To the extent that these activities yield increased revenue, this revenue may not offset the increased expenses we incur. If we do not successfully maintain and enhance our brand or incur substantial expenses in unsuccessful attempts to promote and maintain our brand, our business may not grow, we may have reduced pricing power relative to competitors and we could lose customers and key employees or fail to attract potential customers or talented personnel, all of which would adversely affect our business, results of operations and financial condition. We recognize revenue over the term of our..... over the applicable subscription term. We may acquire or invest in companies, which may divert our management' s attention and result in additional dilution to our stockholders. We may be unable to integrate acquired businesses and technologies successfully or achieve the expected benefits of such acquisitions. Our success depends, in part, on our ability to expand our Unified- CXM platform and grow our business in response to changing technologies, customer demands and competitive pressures. We have in the past, and we may in the future, attempt to do so through strategic transactions, including acquisitions of, or investments in, businesses, technologies, services, products and other assets that we believe could complement, expand or enhance our Unified- CXM platform or otherwise offer growth opportunities. We also may enter into relationships with other businesses to expand our Unified- CXM platform, which could involve preferred or exclusive licenses, additional channels of distribution, discount pricing or investments in other companies. Identifying and negotiating these transactions can be time- consuming, difficult and expensive, and our ability to complete these transactions may often be subject to approvals that are beyond our control. We cannot predict the number, timing or size of these transactions. These transactions, even if announced, may not be completed. Any acquisition, investment or business relationship may result in unforeseen operating difficulties and expenditures. In particular, we may encounter difficulties assimilating or integrating the businesses, technologies, products, personnel or operations of the acquired companies, particularly if the key personnel of the acquired company choose not to work for us, their software is not easily adapted to work with our Unified- CXM platform or we have difficulty retaining the customers of any acquired business due to changes in ownership, management or otherwise. Acquisitions, investments or other business relationships also may disrupt our business, divert our resources and require significant management attention that would otherwise be available for development of our existing business. Moreover, the anticipated benefits of any acquisition, investment or business relationship may not be realized or we may be exposed to unknown risks or liabilities. Our international sales and operations, including our planned business development activities outside of the United States, subject us to additional risks and challenges that can adversely affect our business, results of operations and financial condition. During the year ended January 31, ~~2024~~ **2025**, approximately 41 % of our sales were to customers outside of the Americas. As part of our growth strategy, we expect to continue to expand our international operations, which may include opening additional offices in new jurisdictions and providing our Unified- CXM platform in additional languages and on- boarding new customers outside the United States. Any new markets or countries into which we attempt to

sell subscriptions to our Unified- CXM platform may not be receptive to our business development activities. We currently have sales personnel and sales and customer and product support operations in the United States and certain countries across Europe, the Asia Pacific region and the Americas. We believe that our ability to attract new customers to our Unified- CXM platform and to convince existing customers to renew or expand their use of our Unified- CXM platform is directly correlated to the level of engagement we achieve with our customers in their home countries. To the extent that we are unable to effectively engage with non- U. S. customers, we may be unable to effectively grow in international markets. Our international operations also subject us to a variety of additional risks and challenges, including: • increased management, travel, infrastructure and legal compliance costs associated with having operations and developing our business in multiple jurisdictions; • providing our Unified- CXM platform and operating our business across a significant distance, in different languages, among different cultures and time zones, including the potential need to modify our Unified- CXM platform and products to ensure that they are culturally appropriate and relevant in different countries; • compliance with non- U. S. data privacy, protection and security laws, rules and regulations, including data localization requirements, and the risks and costs of non- compliance; • longer payment cycles and difficulties enforcing agreements, collecting accounts receivable or satisfying revenue recognition criteria, especially in emerging markets; • hiring, training, motivating and retaining highly- qualified personnel, while maintaining our unique corporate culture; • increased financial accounting and reporting burdens and complexities; • longer sales cycle and more time required to educate enterprises on the benefits of our Unified- CXM platform outside of the United States; • requirements or preferences for domestic products; • limitations on our ability to sell our Unified- CXM platform and for our solution to be effective in non- U. S. markets that have different cultural norms and related business practices that de- emphasize the importance of positive customer and employee experiences; • differing technical standards, existing or future regulatory and certification requirements and required features and functionality; • political and economic conditions and uncertainty in each country or region in which we operate and general economic and political conditions and uncertainty around the world; • compliance with laws and regulations for non- U. S. operations, including anti- bribery laws, import and export control laws, tariffs, trade barriers, economic sanctions and other regulatory or contractual limitations on our ability to sell our Unified- CXM platform and develop our business in certain non- U. S. markets, and the risks and costs of non- compliance; • heightened risks of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales arrangements that may impact our financial condition and result in restatements of our consolidated financial statements; • fluctuations in currency exchange rates and related effects on our results of operations; • difficulties in repatriating or transferring funds from or converting currencies in certain countries; • communication and integration problems related to entering new markets with different languages, cultures and political systems; • new and different sources of competition; • differing labor standards, including restrictions related to, and the increased cost of, terminating employees in some countries; • the need for localized subscription agreements; • the need for localized language support and difficulties associated with delivering support, training and documentation in languages other than English; • increased reliance on channel partners; • reduced protection for intellectual property rights in certain non- U. S. countries and practical difficulties of obtaining, maintaining, protecting and enforcing such rights abroad; and • compliance with the laws of numerous foreign taxing jurisdictions, including withholding tax obligations, and overlapping of different tax regimes. Any of these risks and challenges could adversely affect our operations, reduce our revenue or increase our operating costs, each of which could adversely affect our ability to expand our business outside of the United States and thereby our business more generally, as well as our results of operations, financial condition and growth prospects. Compliance with laws and regulations applicable to our international operations substantially increases our cost of doing business. We may be unable to keep current with changes in government requirements as they change from time to time. Failure to comply with these regulations could have adverse effects on our business. In many foreign countries it is common for others to engage in business practices that are prohibited by our internal policies and procedures or U. S. or other regulations applicable to us. Although we have implemented policies and procedures designed to ensure compliance with these laws and policies, there can be no assurance that our employees, contractors, partners and agents will comply with these laws and policies. Violations of laws or our policies by our employees, contractors, partners or agents could result in delays in revenue recognition, financial reporting misstatements, enforcement actions, disgorgement of profits, fines, civil and criminal penalties, damages, injunctions, other collateral consequences and increased costs, including the costs associated with defending against such actions, or the prohibition of the importation or exportation of our Unified- CXM platform and related services, each of which could adversely affect our business, results of operations and financial condition. We face exposure to foreign currency exchange rate fluctuations, and if foreign currency exchange rates fluctuate substantially in the future, our results of operations and financial condition, which are reported in U. S. dollars, could be adversely affected. We conduct our business in countries around the world and a portion of our transactions outside the United States are denominated in currencies other than the U. S. dollar. While we have primarily transacted with customers and vendors in U. S. dollars to date, from time to time we have transacted in foreign currencies for subscriptions to our Unified- CXM platform and may significantly expand the number of transactions with customers that are denominated in foreign currencies in the future. The majority of our international costs are also denominated in local currencies. In addition, our international subsidiaries maintain net assets or liabilities that are denominated in currencies other than the functional operating currencies of these entities. Accordingly, changes in the value of foreign currencies relative to the U. S. dollar can affect our revenue and results of operations due to transactional and translational remeasurements that are reflected in our results of operations. As a result of such foreign currency exchange rate fluctuations, it could be more difficult to detect underlying trends in our business and results of operations. We currently do not maintain a program to hedge transactional exposures in foreign currencies, but we may do so in the future. The future use of hedging instruments may introduce additional risks if we are unable to structure effective hedges with such instruments. There can be no assurance that we will be successful in managing our exposure to currency exchange rate risks, which may adversely affect our business, results of operations and financial condition. Risks Related to Our Intellectual Property Our Unified- CXM

platform utilizes open source software, which may subject us to litigation, require us to re- engineer our Unified- CXM platform or otherwise divert resources away from our development efforts. We use open source software in connection with our Unified- CXM platform and products and operations **, including those products that are currently (or may be) distributed** . Some open source software licenses require users who distribute open source software as part of their software to publicly disclose all or part of the source code to such software or make available any derivative works of the open source code (which may include our modifications or product code into which such open source software has been integrated) on unfavorable terms allowing further modification and redistribution and at no or nominal cost, and we may be subject to such terms. The terms of many open source licenses have not been interpreted by U. S. or foreign courts, and there is a risk that these open source licenses could be construed in a way that imposes unanticipated conditions or restrictions on our ability to commercialize our products. ~~While we monitor~~ **It is possible that** our use of open source software ~~and try~~ **could inadvertently result in, or could be claimed** to **have resulted in** ~~ensure that none is used~~ **use** ~~in a manner~~ that would require us to disclose source code that we have decided to maintain as proprietary or that would otherwise breach the terms or fail to meet the conditions of an open source license or third- party contract ~~, such use could inadvertently occur, or could be claimed to have occurred~~ , in part because open source license terms are often ambiguous **and are not always drafted with certain programming languages in mind** . We could be subject to suits by parties claiming 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 applicable open source licensing terms or alleging that our use of such software infringes, misappropriates or otherwise violates a third party' s intellectual property rights. We may as a result be subject to claims for breach of contract, infringement of intellectual property rights, or indemnity, required to release our proprietary source code, pay damages, **incur additional internal compliance costs,** royalties, or license fees or other amounts, seek licenses, re- engineer our applications, discontinue sales in the event re- engineering cannot be accomplished on a timely basis or take other remedial action that may divert resources away from our development efforts, any of which could adversely affect our business. Any actual or claimed requirement to disclose our proprietary source code or pay damages for breach of the applicable license could harm our business and could help third parties, including our competitors, develop products and services that are similar to or better than ours. Additionally, the use of certain open source software can lead to greater risks than use of third- party commercial software, as open source licensors generally do not provide warranties or controls on the origin of software. There is typically no support available for open source software, and we cannot ensure that the authors of such open source software will implement or push updates to address security risks or will not abandon further development and maintenance. Many of the risks associated with the use of open source software, such as the lack of warranties or assurances of title or performance, cannot be eliminated, and could, if not properly addressed, negatively affect our business. **While we do keep track of** ~~We have processes to help alleviate these risks, including a review process for screening requests from~~ our ~~developers for the~~ use of open **-** source software, ~~but~~ we cannot be sure that all open source software is identified ~~or submitted for approval~~ prior to use in our products and services. Any of these risks could be difficult to eliminate or manage, and, if not addressed, could have an adverse effect on our business, financial condition, and results of operations. Our success and ability to compete depend in part upon our ability to obtain, maintain, protect, defend and enforce our intellectual property. As of January 31, ~~2024~~ **2025** , we owned 38 U. S. issued patents and 10 pending non- provisional or provisional U. S. patent applications. We rely on a combination of patent, copyright, trademark and trade secret laws in the United States and internationally, as well as technological measures and contractual provisions, such as confidentiality or license agreements with our employees, customers, partners, and other third parties, to establish and protect our brand, maintain our competitive position and protect our intellectual property rights from infringement, misappropriation or other violation. However, the steps we take to protect our intellectual property rights may be inadequate or ineffective, and our intellectual property may be challenged, invalidated, narrowed in scope or rendered unenforceable through administrative processes, including re- examination, inter partes review, interference and derivation proceedings and equivalent proceedings in foreign jurisdictions (e. g., opposition proceedings) or litigation. The steps we take to protect our intellectual property rights may not be sufficient to effectively prevent third parties from infringing, misappropriating or otherwise violating our intellectual property or to prevent unauthorized disclosure or unauthorized use of our trade secrets or other confidential information. We cannot guarantee that any of our pending applications will issue or be approved or that our existing and future intellectual property rights will be sufficiently broad to protect our proprietary technology. Additionally, effective trademark, copyright, patent and trade secret protection may not be available in every country in which we conduct business, and we may fail to maintain or be unable to obtain adequate protections for certain of our intellectual property rights in such foreign countries. Further, intellectual property law, including statutory and case law, particularly in the United States, is constantly developing, and any changes in the law could make it harder for us to enforce our rights. Failure to comply with applicable procedural, documentary, fee payment and other similar requirements with the United States Patent and Trademark Office and various similar foreign governmental agencies could result in abandonment or lapse of the affected patent, trademark or application. If this occurs, our competitors might be more successful in their efforts to compete with us. Effective protection of intellectual property rights is expensive and difficult to maintain, both in terms of application and registration costs, as well as the costs of defending and enforcing those rights. We attempt to protect our intellectual property, technology, and confidential information in part through confidentiality, non- disclosure and invention assignment agreements with our employees, consultants, contractors, corporate collaborators, advisors and other third parties who develop intellectual property on our behalf or with whom we share information. However, we cannot guarantee that we have entered into such agreements with each party who has developed intellectual property on our behalf and each party that has or may have had access to our confidential information, know- how and trade secrets. These agreements may be insufficient or breached, or may not effectively prevent unauthorized access to or unauthorized use, disclosure, misappropriation or reverse engineering of, our confidential information, intellectual property, or technology. There can be no assurance that these agreements will be self- executing or otherwise provide meaningful protection

for our trade secrets or other intellectual property or proprietary information. Moreover, these agreements may not provide an adequate remedy for breaches or the unauthorized use or disclosure of our confidential information or technology or infringement of our intellectual property. Enforcing a claim that a party illegally disclosed or misappropriated a trade secret or know- how is difficult, expensive, and time- consuming, and the outcome is unpredictable. In addition, trade secrets and know- how can be difficult to protect, and some courts inside and outside the United States are less willing or unwilling to protect trade secrets and know- how. If any of our trade secrets were to be lawfully obtained or independently developed by a competitor or other third party, we would have no right to prevent them from using that technology or information to compete with us, and our competitive position would be materially and adversely harmed. The loss of trade secret protection could make it easier for third parties to compete with our products and services by copying functionality. Additionally, individuals not subject to invention assignment agreements may make adverse ownership claims to our current and future intellectual property, and, to the extent that our employees, independent contractors or other third parties with whom we do business use intellectual property owned by others in their work for us, disputes may arise as to the rights in related or resulting know- how and inventions. There is also a risk that we do not establish an unbroken chain of title from inventors to us. An inventorship or ownership dispute could arise that may permit one or more third parties to practice or enforce our intellectual property rights, including possible efforts to enforce rights against us. Additionally, errors in inventorship or ownership can sometimes also impact priority claims, and if we were to lose our ability to claim priority for certain patent filings, intervening art or other events may preclude us from issuing patents. Moreover, policing unauthorized use of our technologies, trade secrets, and intellectual property may be difficult, expensive and time- consuming, particularly in foreign countries where the laws may not be as protective of intellectual property rights as those in the United States and where mechanisms for enforcement of intellectual property rights may be weak or inadequate. Furthermore, we may not always detect infringement, misappropriation or other violation of our intellectual property rights, and any infringement, misappropriation or other violation of our intellectual property rights, even if successfully detected, prosecuted and enjoined, could be costly to deal with and could harm our business. In addition, there can be no assurance that our intellectual property rights will be sufficient to protect against others offering products or services that are substantially similar to ours and competing with our business, and third parties, including our competitors, may independently develop similar technology, duplicate our services or design around our intellectual property and, in such cases, we may not be able to successfully assert our intellectual property rights against such parties. Further, our contractual arrangements may not effectively prevent disclosure of our trade secrets or confidential information or provide an adequate remedy in the event of unauthorized disclosure of our trade secrets or confidential information, and we may be unable to detect the unauthorized use of, or take appropriate steps to enforce, such trade secrets, confidential information and other intellectual property rights. Any of the foregoing could adversely affect our business, results of operations and financial condition. In order to protect our intellectual property rights, we may be required to spend significant resources to monitor and protect these rights. Litigation brought to protect and enforce our intellectual property rights could be costly, time- consuming and distracting to management, and could result in the impairment or loss of portions of our intellectual property. Uncertainties resulting from the initiation and continuation of patent litigation or other proceedings could have a material adverse effect on our ability to compete in the marketplace. Furthermore, our efforts to enforce our intellectual property rights may be met with defenses, counterclaims and countersuits attacking the validity and enforceability of our intellectual property rights, which could result in the impairment or loss of portions of our intellectual property portfolio. An adverse determination of any litigation proceedings could put our intellectual property at risk of being invalidated or interpreted narrowly and could put our related patents, pending patent applications and trademark filings at risk of being invalidated, not issuing or being cancelled. Furthermore, because of the substantial amount of discovery required in connection with intellectual property litigation, there is a risk that some of our confidential or sensitive information could be compromised by disclosure in the event of litigation. In addition, during the course of litigation there could be public announcements of the results of hearings, motions or other interim proceedings or developments. Despite our efforts, we may not be able to prevent third parties from infringing, misappropriating or otherwise violating, or from successfully challenging, our intellectual property rights. If securities analysts or investors perceive these results to be negative, it could have a substantial adverse effect on the price of our Class A common stock. Such litigation or proceedings could substantially increase our operating losses and reduce the resources available for development activities or any future sales, marketing or distribution activities. Our failure to obtain, maintain, protect, defend and enforce our intellectual property rights could adversely affect our brand and business, financial condition and results of operations. We may face claims by third parties alleging infringement, misappropriation or other violation of their intellectual property, trade secrets or proprietary rights. There is considerable patent and other intellectual property development activity in our industry and companies in the technology industry frequently enter into litigation based on allegations of infringement, misappropriation or other violations of intellectual property rights. Our future success depends in part on our ability to develop and commercialize our products and services without infringing, misappropriating or otherwise violating the intellectual property and proprietary rights of others. From time to time, we have received and may in the future receive claims from third parties, including our competitors, alleging that our Unified- CXM platform and underlying technology infringe, misappropriate or otherwise violate such third party' s intellectual property rights, including their trade secrets, and we may be found to be infringing upon such rights. For example, on February 25, 2022, we agreed to settle all outstanding claims with Opal Labs Inc. (" Opal ") with respect to Opal' s complaints alleging breach of contract and violation of Oregon' s Uniform Trade Secrets Act, among other claims, and, on March 1, 2022, the court dismissed those claims with prejudice. **We** ~~The Company~~ and Opal finalized the settlement on March 15, 2022, and it was paid on March 30, 2022. As we face increasing competition and become increasingly high profile, the possibility of receiving a larger number of intellectual property claims against us grows. It is possible that we may be unsuccessful in such proceedings, resulting in a loss of some portion or all of our patent rights. Any claims or litigation, regardless of their merit, could cause us to incur significant expenses, pay substantial amounts in costs or damages, ongoing

royalty or license fees or other payments, or could prevent us from offering all or aspects of our Unified- CXM platform or using certain technologies, require us to re- engineer all or a portion of our Unified- CXM platform, force us to implement expensive workarounds or re- designs, distract management from our business or require that we comply with other unfavorable terms. If any of our technologies, products or services are found to infringe, misappropriate or violate a third party' s intellectual property rights, we may seek to obtain a license under such third party' s intellectual property rights in order to bring an end to certain claims or actions asserted against us to continue commercializing or using such technologies, products and services. However, we may not be able to obtain such a license on commercially reasonable terms or at all. Even if we were able to obtain a license, it could be non- exclusive, thereby giving our competitors and other third parties access to the same technologies licensed to us, and it could require us to make substantial licensing and royalty payments. Any litigation also may involve patent holding companies or other adverse patent owners that have no relevant solution revenue, and, therefore, our patent portfolio may provide little or no deterrence, as we would not be able to assert our patents against such entities or individuals. Such " non- practicing entities " and other intellectual property rights holders may attempt to assert intellectual property claims against us or seek to monetize the intellectual property rights they own to extract value through licensing or other settlements. We have in the past and may in the future be requested to and / or obligated to indemnify our customers or business partners in connection with any such litigation and to obtain licenses or refund subscription fees, which could further exhaust our resources. Even if we were to prevail in the event of claims or litigation against us, any claim or litigation regarding our technology or intellectual property, with or without merit, could be unpredictable, costly and time- consuming, and divert significant resources and the attention of our management and other employees from our business operations. Such disputes also could disrupt our Unified- CXM platform and products, which would adversely impact our client satisfaction and ability to attract customers. In the case of infringement, misappropriation or other violation caused by technology that we obtain from third parties, any indemnification or other contractual protections we obtain from such third parties, if any, may be insufficient to cover the liabilities we incur as a result of such infringement or misappropriation. In a patent infringement claim against us, we may assert, as a defense, that we do not infringe the relevant patent claims, that the patent is invalid or both. The strength of our defenses will depend on the patents asserted, the interpretation of these patents, and our ability to invalidate the asserted patents. However, we could be unsuccessful in advancing non- infringement or invalidity arguments in our defense. In the United States, issued patents enjoy a presumption of validity, and the party challenging the validity of a patent claim must present clear and convincing evidence of invalidity, which is a high burden of proof. Conversely, the patent owner need only prove infringement by a preponderance of the evidence, which is a lower burden of proof. We also may be unaware of the intellectual property rights of others that may cover some or all of our technology. Because patent applications can take years to issue and are often afforded confidentiality for some period of time, there may currently be pending applications, unknown to us, that later result in issued patents that could cover one or more of our products. If we are required to make substantial payments or undertake any of the other actions noted above as a result of any intellectual property infringement, misappropriation or violation claims against us, such payments, costs or actions could have a material adverse effect on our competitive position, business, financial condition and results of operations. Indemnity and other provisions in various agreements potentially expose us to substantial liability for intellectual property infringement and other losses. Our agreements with customers and other third parties may include indemnification or other provisions under which we agree to indemnify or otherwise be liable to such third parties for losses suffered or incurred as a result of claims of intellectual property infringement, misappropriation or other violation, damages caused by us to property or persons or other liabilities relating to or arising from our Unified- CXM platform or our acts or omissions. We have in the past and may in the future receive indemnification requests from our customers related to such claims. In addition, customers typically require us to indemnify or otherwise be liable to them for breach of confidentiality or failure to implement adequate security measures with respect to their data stored, transmitted or processed by our Unified- CXM platform. The terms of these contractual provisions often survive termination or expiration of the applicable agreement. Large indemnity payments or damage claims from contractual breach could harm our business, results of operations and financial condition. Although we generally attempt to contractually limit the scope of our liability with respect to such obligations, we are not always successful, and we may incur substantial liability related to them. Any dispute with a customer with respect to such obligations could have adverse effects on our relationship with that customer and other current and prospective customers, reduce demand for our Unified- CXM platform and harm our business, financial condition and results of operations. Further, certain of our customer agreements contain provisions permitting the customer to become a party to, or a beneficiary of, a source code escrow agreement under which we place the proprietary source code for certain of our solutions in escrow with a third party. Under these source code escrow agreements, our source code may be released to the customer upon the occurrence of specified events, such as in situations of our bankruptcy or insolvency or our failure to support or maintain our solutions. Disclosing the content of our source code may limit the intellectual property protection we can obtain or maintain for our source code or our solutions containing that source code and may facilitate intellectual property infringement, misappropriation or other violation claims against us. Following any such release, we cannot be certain that customers will comply with the restrictions on their use of the source code and we may be unable to monitor and prevent unauthorized disclosure of such source code by customers. Additionally, following any such release, customers may be able to create derivative works based on our source code and may own such derivative works. Any increase in the number of people familiar with our source code as a result of any such release also may increase the risk of a successful hacking attempt. Each of these could have a material adverse effect on our business, financial condition and results of operations. Risks Related to Litigation, Regulatory Compliance and Governmental Matters Our business and operations could be negatively affected **by** ~~if we become subject to~~ any **pending or future** securities litigation or stockholder activism. ~~Our business~~ **We are,** and **may** ~~operations could be negatively affected if we~~ become **in the future,** subject to ~~any~~ securities ~~litigation~~ **class actions, derivative suits or other securities- related legal actions.** ~~or~~ **For example, in August 2024, a putative securities class action was filed against us and certain of our officers alleging violations of the**

federal securities laws for allegedly making false and misleading statements. On March 18, 2025, a stockholder ~~activism~~ **derivative action was filed** , **purporting** ~~which could cause us~~ to ~~incur significant expenses, hinder~~ **bring claims on behalf of the Company against certain of our current and former directors and officers for alleged violations of the federal securities laws and breaches of** ~~the~~ **their fiduciary duties, among** ~~execution of our business and growth strategy and impact the~~ **other** ~~price of our~~ **claims, in relation to substantially the same factual allegations as those made in the securities** ~~Class~~ **class action** ~~A common stock~~ . In the past, securities class action litigation **have** often ~~has~~ been brought against a company following a decline in the market price of its securities. In addition, stockholder activism, which could take many forms and arise in a variety of situations, has been increasing recently, and new universal proxy rules could significantly lower the cost and further increase the ease and likelihood of stockholder activism. This risk is especially relevant for us because technology companies have experienced significant stock price volatility in recent years. Volatility in our stock price or other reasons may in the future cause us to become the target of securities litigation or stockholder activism. Securities litigation and stockholder activism, including potential proxy contests, could result in substantial costs, including significant legal fees and other expenses, and divert our management and board of directors' attention and resources from our business. Additionally, securities litigation and stockholder activism could give rise to perceived uncertainties as to our future, adversely affect our relationships with customers and business partners, adversely affect our reputation, and make it more difficult to attract and retain qualified personnel. Our stock price could also be subject to significant fluctuation or otherwise be adversely affected by the events, risks and uncertainties of any securities litigation and stockholder activism. **Any claims or litigation, even if fully indemnified or insured, could adversely affect our relationships with customers and business partners, damage our reputation, decrease customer demand for our services and make it more difficult to attract and retain qualified personnel, making it more difficult for us to compete effectively. In addition, lawsuits or legal claims involving us may increase our insurance premiums, deductibles or co- insurance requirements or otherwise make it more difficult for us to maintain or obtain adequate insurance coverage on acceptable terms, if at all. Furthermore, while we maintain insurance for certain potential liabilities, such insurance does not cover all types and amounts of potential liabilities and is subject to various exclusions, as well as caps on amounts recoverable. Even if we believe that a claim is covered by insurance, insurers may dispute our entitlement to recovery for a variety of potential reasons, which may affect the timing and, if the insurers prevail, the amount of our recovery. Our exposure under these matters may also include our indemnification obligations, to the extent that we have any, to current and former officers and directors against losses incurred in connection with these matters, including reimbursement of legal fees and other expenses. As a result, pending or future lawsuits involving us, or our officers or directors, could have a material adverse effect on our business, reputation, financial condition, results of operations, liquidity and the trading price of our Class A common stock.** We are subject to governmental export and import controls and economic sanctions laws and regulations that could impair our ability to compete in international markets and subject us to liability if we are not in full compliance with applicable laws. Our business activities are subject to various restrictions under U. S. export and similar laws and regulations, including the United States Department of Commerce' s Export Administration Regulations and various economic and trade sanctions regulations administered by the United States Treasury Department' s Office of Foreign Assets Controls. The U. S. export control laws and economic sanctions laws include restrictions or prohibitions on the sale or supply of certain products and services to certain embargoed or sanctioned countries, governments, persons and entities. In addition, we may incorporate encryption technology into certain of our offerings, and encryption offerings and the underlying technology may be exported outside of the United States only with the required export authorizations, including by license, and we cannot guarantee that any required authorization will be obtained. If we are found to be in violation of U. S. economic sanctions or export control laws, it could result in substantial fines and penalties for us and for the individuals working for us. We also may experience other adverse effects, including reputational harm and loss of access to certain markets. In addition, various countries regulate the import of certain technology and have enacted or could enact laws that could limit our ability to provide our customers access to our Unified- CXM platform or could limit our customers' ability to access or use our Unified- CXM platform in those countries. Changes in our Unified- CXM platform or future changes in export and import regulations may prevent our customers with international operations from utilizing our Unified- CXM platform globally or, in some cases, prevent the export or import of our Unified- CXM platform to certain countries, governments or persons altogether. Any decreased use of our Unified- CXM platform or limitation on our ability to export or sell our Unified- CXM platform could adversely affect our business, results of operations and financial condition. Failure to comply with anti- bribery, anti- corruption and anti- money laundering laws could subject us to penalties and other adverse consequences. We are subject to the U. S. Foreign Corrupt Practices Act of 1977, as amended (the " FCPA "), the U. K. Bribery Act and other anti- corruption, anti- bribery and anti- money laundering laws in the jurisdictions in which we do business, both domestic and abroad. These laws generally prohibit us and our employees from improperly influencing government officials or commercial parties in order to obtain or retain business, direct business to any person or gain any advantage. The FCPA, U. K. Bribery Act and other applicable anti- bribery and anti- corruption laws also may hold us liable for acts of corruption and bribery committed by our third- party business partners, representatives and agents. In addition to our own sales force, we leverage third parties to sell our products and conduct our business abroad. We and our third- party business partners, representatives and agents may have direct or indirect interactions with officials and employees of government agencies or state- owned or affiliated entities and we may be held liable for the corrupt or other illegal activities of these third- party business partners and intermediaries, our employees, representatives, contractors, channel partners and agents, even if we do not explicitly authorize such activities. These laws also require that we keep accurate books and records and maintain internal controls and compliance procedures designed to prevent any such actions. While we have policies and procedures to address compliance with such laws, we cannot assure you that our employees and agents will not take actions in violation of our policies or applicable law, for which we may be ultimately held responsible and our exposure for violating these laws increases as our

international presence expands and as we increase sales and operations in foreign jurisdictions. Any violation of the FCPA, U. K. Bribery Act or other applicable anti- bribery, anti- corruption laws and anti- money laundering laws could result in whistleblower complaints, adverse media coverage, investigations, imposition of significant legal fees, loss of export privileges, severe criminal or civil sanctions or suspension or debarment from U. S. government contracts, substantial diversion of management' s attention, a decline in the market price of our Class A common stock or overall adverse consequences to our reputation and business, all of which may have an adverse effect on our results of operations and financial condition. Our business could be adversely ~~impacted~~ **affected** by changes in laws and regulations related to the Internet or changes in access to the Internet generally. The future success of our business depends upon the continued use of the Internet as a primary medium for communication, business applications and commerce. Federal or state government bodies or agencies have in the past adopted, and may in the future adopt, laws or regulations affecting the use of the Internet as a commercial medium. Legislators, regulators or government bodies or agencies also may make legal or regulatory changes or interpret or apply existing laws or regulations that relate to the use of the Internet in new and materially different ways. Changes in these laws, regulations or interpretations could require us to modify our Unified- CXM platform in order to comply with these changes, to incur substantial additional costs or divert resources that could otherwise be deployed to grow our business, or expose us to unanticipated civil or criminal liability, among other things. In addition, **federal and state** government agencies and private organizations have imposed, and may in the future impose, additional taxes, fees or other charges for accessing the Internet or commerce conducted via the Internet. Internet access is frequently provided by companies that have significant market power and could take actions that degrade, disrupt or increase the cost of our customers' use of our Unified- CXM platform, which could negatively impact our business. In December 2017, the Federal Communications Commission (" FCC ") ~~, voted to repeal~~ **repealed** its **2015** " ~~net~~ **network** neutrality " ~~Open Internet~~ rules, effective June 2018. The **2015 network neutrality** rules were designed to ensure that all online content ~~is~~ **and services were** treated the same by internet service providers ~~and other companies that provide broadband services. The FCC' s new rules, which took effect on June 11, 2018, repealed the neutrality obligations imposed by the Open Internet rules~~ and granted providers of broadband internet access services greater freedom to make changes to their services, including, potentially, changes that may discriminate against or harm our business. In ~~October~~ **April** ~~2023~~ **2024** , the FCC **adopted an order that** ~~voted to begin the process of reinstating~~ substantially ~~all~~ **reinstated the 2015 rules, but the U. S. Court** of **Appeals for the Sixth Circuit overturned the FCC' s decision on January 2, 2025, which means that** ~~the~~ **there** ~~net~~ **is no federal regulation requiring network** neutrality ~~rules~~ **. A number of states have adopted or are adopting or considering legislation or executive actions** that **would regulate** ~~had been in place prior to~~ the ~~2018 repeal~~ **conduct of broadband providers. For example, California and Vermont have state- level requirements in effect, and New York is considering similar legislation** . We cannot predict the actions that the FCC may take, whether any new FCC order or state initiatives regulating providers will be modified, overturned, or vacated by legal action, federal legislation, or the FCC itself, or the degree to which ~~further~~ **additional federal or state** regulatory action ~~, ,~~ or inaction ~~, ,~~ may adversely affect our business. **We** ~~Should the net neutrality rules not be reinstated, we~~ could incur greater operating expenses or our customers' use of our Unified- CXM platform could be adversely affected, either of which could harm our business and results of operations. These developments could limit the growth of Internet- related commerce or communications generally or result in reductions in the demand for Internet- based platforms and services such as ours, increased costs to us or the disruption of our business. In addition, as the Internet continues to experience growth in the ~~numbers~~ **number** of users, frequency of use and amount of data transmitted, the use of the Internet as a business tool could be adversely affected due to delays in the development or adoption of new standards and protocols to handle increased demands of Internet activity, security, reliability, cost, ease- of- use, accessibility and quality of service. The performance of the Internet and its acceptance as a business tool has been adversely affected by data security and privacy issues, and the Internet has experienced a variety of outages and other degradations as a result of damage to portions of its infrastructure. If the use of the Internet generally, or our Unified- CXM platform specifically, is adversely affected by these or other issues, we could be forced to incur substantial costs, demand for our Unified- CXM platform could decline and our results of operations and financial condition could be harmed. **Our business could be adversely impacted by laws and regulations related to the telecommunications industry. We provide certain communications and voice services that are or could become subject to existing or potential domestic or international regulations around telecommunications. For example, we are registered as an interconnected Voice Over Internet Protocol (" VoIP ") provider in the United States, which subjects us to the FCC' s rules and regulations applicable to VoIP providers such as filings and regulatory assessments (including contributions to FCC- mandated funds), call authentication requirements, access to emergency services, requirements around the provision or portability of phone numbers, data privacy, and law enforcement access laws. We may seek to expand business activities to new jurisdictions, which could subject us to new or increased regulations, increase compliance costs or limit the level of services we offer, each of which could affect our business strategies and potential customer base. In addition, existing and future laws and regulations could limit our ability to make telephone numbers available to customers who request them. Legislators or the agencies may expand the scope of our regulatory obligations or limit our rights at any time. If we do not comply with any current or future regulations that apply to our business, we could be subject to substantial fines and penalties, we may have to restructure our product offerings, exit certain markets, or raise the price of our products, any of which could ultimately harm our business and results of operations. Any enforcement action by the regulators, which may be a public process, would hurt our reputation in the industry, possibly impair our ability to sell our services to our customers and harm our business.** Risks Related to Privacy, Information Technology and Cybersecurity Interruptions in availability or suboptimal performance associated with our technology and infrastructure may adversely affect our business, results of operations and financial condition. We seek to maintain the integrity and availability of our products and confidentiality of our confidential information through certain controls, such as business continuity and disaster recovery plans, redundant designs of operational systems and

processes, training and availability of key employees, contractual and technical assurances by our third- party service providers to maintain their services to us, regular tests and audits of critical systems and plans, capacity planning for current and future system and process needs, enterprise risk management, and periodic review of our plans. Notwithstanding these efforts, we cannot ensure that our systems or those of ~~our~~ **the** third ~~- party partners~~ - **parties with whom we work** are not or will not be vulnerable to disruptions from natural or man- made disasters or other security incidents. We are exposed to threats and resulting risks that may result in a significant disruption of our ability to deliver our products to our customers. Our continued growth, brand, reputation and ability to attract and retain customers depend in part on the ability of our customers to access our Unified- CXM platform at any time and within an acceptable amount of time. Our Unified- CXM platform is proprietary, and we are dependent on the expertise and efforts of members of our engineering, operations and software development teams for its continued performance. We have experienced, and may in the future experience, service disruptions, outages and other performance problems due to a variety of factors, including infrastructure changes, introductions of new functionality, human or software errors, capacity constraints due to an overwhelming number of users accessing our Unified- CXM platform concurrently and denial of service attacks or other security- related incidents. Frequent or persistent interruptions in our products and services could cause customers to believe that our products and services are unreliable, leading them to **limit or reduce their use of our products,** switch to our competitors or ~~to~~ avoid our products and services. Additionally, our insurance policies may be insufficient to cover a claim made against us by any such customers affected by any errors, defects or other infrastructure problems. In some instances, we may not be able to rectify, remediate or even identify the cause or causes of these performance issues within an acceptable period of time. It may become increasingly difficult to maintain and improve our performance, especially during peak usage times, as our Unified- CXM platform becomes more complex and our user traffic increases. If our Unified- CXM platform is unavailable or if users are unable to access our Unified- CXM platform within a reasonable amount of time, or at all, our business, results of operations and financial condition would be adversely affected. Moreover, some of our customer agreements include performance guarantees and service- level standards that obligate us to provide credits or termination rights in the event of a significant disruption in the functioning of our Unified- CXM platform. To the extent that we do not effectively address capacity constraints, upgrade our systems and data centers as needed and continually develop our technology and network architecture to accommodate actual and anticipated changes in technology or an increased user base, we may experience service interruptions and performance issues, which may result in a disruption of our products, delay the development of new products and features, result in a loss of current and future revenue, result in negative publicity and harm to our reputation, require us to pay significant penalties or fines or subject us to litigation, claims or other disputes, any of which could have an adverse effect on our business, results of operations and financial condition. In the ordinary course of business, we collect, receive, store, process, generate, use, transfer, disclose, make accessible, protect, secure, dispose of, transmit ~~and~~ **,** share **and conduct other activities with** (which we collectively refer to as " process ") proprietary and confidential data, including personal data, intellectual property, and trade secrets, of ours or our customers (collectively, " confidential information "). Additionally, our customers can utilize our Unified- CXM platform to process confidential information ~~of~~ **or personal data relating to** their employees, customers, partners and other individuals. Our data processing activities subject us to numerous **global** data privacy and security obligations, such as various laws, regulations, guidance, industry standards, external and internal privacy and security policies, contracts, and other obligations that govern the processing of confidential information by us and on our behalf. In the United States, federal, state, and local governments have enacted numerous data privacy and security laws, including data breach notification laws, personal data privacy laws, and consumer protection laws (such as Section 5 of the Federal Trade Commission Act), and other laws, including wiretapping laws. For example, ~~various~~ **some** privacy laws and other obligations ~~may~~ require us **or our customers** to obtain ~~consents~~ - **consent** to process personal data in certain circumstances. ~~For example, some~~ **Some** of our data processing practices may be challenged under wiretapping laws, as we obtain customer information from third parties through various methods, including chatbot and session replay providers, or via third- party marketing pixels. **In addition, we must comply with the FCC' s regulations that require us to protect private customer information about their use of telecommunications services, known as customer proprietary network information.** Our **, or the third parties with whom we work,** inability or failure to ~~do so~~ **adhere to applicable requirements** could result in adverse consequences, including class action litigation ~~and~~ **,** mass arbitration demands **and statutory fines for noncompliance** . In the past few years, numerous U. S. states ~~— including California, Virginia, Colorado, Connecticut, and Utah —~~ have enacted comprehensive privacy laws that impose certain obligations on covered businesses, including providing specific disclosures in privacy notices and affording residents with certain rights concerning their personal data. As applicable, such rights may include the right to access, correct, or delete certain personal data, and to opt- out of certain data processing activities, such as targeted advertising, profiling, and automated decision- making **, which, even if not directly applicable to Sprinklr as a data processor, may be applicable to our customers** . The exercise of these rights may impact our business and ability to provide our products and services. These state laws also allow for statutory fines for noncompliance. For example, under the California Consumer Privacy Act of 2018 ~~, as amended by the California Privacy Rights Act of 2020~~ (~~collectively,~~ " CCPA ") noncompliance **carries** ~~may carry~~ fines **and** ~~of up to $ 7, 500 per intentional violation; the CCPA~~ also allows for a private right of action for certain data breaches. These laws, as well as other laws or regulations relating to data privacy and security, particularly any new or modified laws or regulations that require enhanced protection of certain types of data or new obligations with regard to data retention, transfer or disclosure, may result in further uncertainty with respect to data privacy and security issues, and will require us to incur additional resource, costs and expenses in an effort to comply. The enactment of ~~such~~ **various** laws has prompted similar legislative developments in other states, which ~~could~~ **has** ~~create~~ **created** ~~the potential for~~ a patchwork of overlapping **nuanced** ~~but different~~ state laws, as certain state laws may be more stringent, broader in scope or offer greater individual rights with respect to personal data than federal, foreign or other state laws, which ~~may~~ complicate compliance efforts. The federal government is also **still** considering comprehensive privacy

legislation. In addition, as we continue to expand our business activities, we are accessing additional types and greater volumes of potentially confidential **or sensitive** information that may subject us to additional privacy and security laws and obligations. For example, in certain limited instances, we ~~may~~ **have** ~~agree~~ **agreed** with specific customers to permit the exchange of protected health information through certain approved platform components. Our access to protected health information for specific agreed **upon** use cases on behalf of those customers that are covered entities and therefore subject to the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act (collectively, " HIPAA "), may subject us to HIPAA' s specific requirements relating to the privacy, security, and transmission of protected health information. To the extent that we **are or may** become subject to HIPAA, our failure to comply could result in significant penalties. Additionally, to the extent that additional customers with whom we did not agree to permit the exchange of protected health information through our platforms in their capacity as covered entities nonetheless ~~provide~~ **input or allow** such information **within the platform** in violation of their contractual obligations with us, we could also be subject to additional compliance risks. Similar privacy, security, and transmission obligations may apply to us outside the United States if we process health information and other categories of **sensitive or** confidential information **knowingly or unknowingly,** and our failure to comply could result in significant penalties. As **we expand into more regulated industries, there may be additional obligations regarding the types of data in scope, and higher risk due to the sensitivity and potential impact of exposure. As** another example, we **enable the** ~~process~~ **processing** ~~an increasing amount~~ of credit card data **through our Secure Forms module** , and we have entered contractual relationships requiring us to comply with the Payment Card Industry Data Security Standard (" PCI DSS "). The PCI DSS requires companies to adopt certain measures to ensure the security of cardholder information, including using and maintaining firewalls, adopting proper password protections for certain devices and software, and restricting data access. Noncompliance with PCI- DSS can result in penalties ranging from $ 5, 000 to $ 100, 000 per month by credit card companies, litigation, damage to our reputation, and revenue losses. Outside of the United States, an increasing number of laws, regulations, and industry standards apply to data privacy and security. Some examples of ~~these~~ laws **that apply to our processing of personal data** include the European Union' s General Data Protection Regulation (" EU GDPR "), the United Kingdom' s GDPR (" UK GDPR " and, together with EU GDPR, " GDPR "), Brazil' s General Data Protection Law (Lei Geral de Proteção de Dados Pessoais) (Law No. 13, 709 / 2018), China' s Personal Information Protection Law, India' s Digital Personal Data Protection Act, and Japan' s **Act on the** Protection of Personal Information. These laws all impose strict requirements for processing personal data. For example, noncompliance with the EU GDPR carries fines of up to the greater of € 20 million or 4 % of global annual turnover (and under the UK GDPR, up to the greater of £ 17. 5 million or 4 % of global annual turnover) and can result in data processing bans, other administrative penalties and litigation brought by classes of data subjects or consumer protection organizations authorized at law to represent their interests, together with associated damage to our reputation. Europe and other jurisdictions have **proposed or** enacted laws requiring data to be localized in some limited circumstances or limiting the transfer of personal data to other countries. In ~~particular~~ **addition, some customers have internal policy requirements which may differ from, or be more burdensome than, applicable regulations. For example** , European and other data protection laws, including the GDPR, **place some** ~~restrict~~ **restrictions on** the ability of companies to **freely** transfer personal data to ~~the United States and other~~ countries **deemed to be inadequate for privacy purposes** , and there are **fairly** rigorous restrictions regarding transfers of personal data from China. Other jurisdictions may also adopt stringent data localization and cross- border data transfer requirements and, in ~~some~~ **many** circumstances, these may be requirements outside of the scope of privacy law, including industry- specific or national security requirements. **With respect to data transfers under the GDPR,** ~~Although~~ **although** there are currently various mechanisms that may be used to enable the transfer of personal data from the European Economic Area (" EEA ") and UK to the United States in compliance with the law, such as the EU- US Data Privacy Framework and the UK extension thereto (to which we are an active participant) and the EU' s standard contractual clauses, these mechanisms ~~are~~ **continue to be** subject to legal challenges, and there is no continued assurance that we can satisfy or rely on these measures to lawfully transfer personal data to the United States or other countries with " inadequate " data protection regimes without the potential for future challenge. If there is no lawful manner for us to transfer personal data from the EEA, the UK, or other jurisdictions ~~,~~outside of the origin territory, or if the requirements for a legally- compliant transfer are too onerous, we could face significant adverse consequences, including the prohibition on further transfers **(including remote access by employees in support teams in certain regions)** , the interruption or degradation of our operations, the need to relocate part of or all of our business or data processing activities to other jurisdictions at significant expense, increased exposure to regulatory actions, substantial fines and penalties, the inability to transfer data and work with partners, vendors and other third parties, and injunctions against our processing or transferring of personal data necessary to operate our business. Additionally, companies that transfer personal data out of the EEA and UK to other jurisdictions, particularly to the United States, ~~are~~ **can be** subject to increased scrutiny from regulators, individual litigants, and activist groups. **Regulators in the United States, such as the U. S. Department of Justice, also are increasingly scrutinizing certain personal data transfers and have proposed and enacted certain data localization requirements, such as, for example, the Biden Administration' s executive order Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government- Related Data by Countries of Concern.** We **are or** may ~~also~~ become **directly or indirectly** subject to new laws in the EEA that regulate cybersecurity and non- personal data, such as the ~~European~~ **EU** Data Act **, the EU Digital Operational Resilience Act (DORA) or the so- called " EU NIS2 Directive** . **"** Depending on how ~~these~~ **new** laws are **implemented and** interpreted, we may have to adapt our business practices **, contractual arrangements** and products to comply with such obligations. UK and EEA data privacy regulations in relation to electronic communications also require opt- in consent to send **certain unsolicited** marketing emails or other electronic communications to individuals or for the use of cookies and the data obtained using cookies and similar technologies for advertising, analytics and certain other purposes – activities on which our products and marketing strategies rely. Enforcement

of these requirements has increased, and a new regulation proposed in the **EU** ~~European Union~~, known as the ePrivacy Regulation, makes these requirements, as well as requirements around tracking technologies, such as cookies, more stringent and increases the penalties for violating them. Such restrictions could increase our exposure to regulatory enforcement action, increase our compliance costs, and adversely affect our business. We sometimes rely on **certain** data obtained from third- party data suppliers, and the sale of data to third parties has become subject to increased regulatory scrutiny. Therefore, obtaining information from third parties carries risk to us as a data purchaser **and onward provider to our customers**. Regulators are increasingly scrutinizing the activities of third- party data suppliers, as well as those using the data from those third parties, and laws in the United States (including the CCPA and California Delete Act) and other jurisdictions, such as Europe (including GDPR **,** and the ePrivacy Directive), are likewise regulating such activity. These laws pose additional, material compliance risks to such suppliers, and these suppliers may not be able to supply us with personal data in compliance with these laws. Such laws may make it difficult for our suppliers to provide the data as the costs associated with the data materially increase. For example, some data suppliers are required to register as data brokers under California, Vermont, Texas and Oregon law and file reports with regulators, which exposes them to increased scrutiny. Additionally, the California Delete Act requires the California Privacy Protection Agency to establish by January 1, 2026 a mechanism to allow California consumers to submit a single, verifiable request to delete all of their personal data held by all registered data brokers and their service providers. Moreover, third- party data suppliers have recently been subject to increased litigation under various claims of violating certain state privacy laws. These laws and challenges may make it so difficult for our suppliers to provide data to us that the costs associated with the data materially increase or may materially decrease the availability of data that our data suppliers can provide us. In addition, we may face compliance risks and limitations on our ability to use certain data provided by our third- party suppliers if those suppliers have not complied with applicable privacy laws, ~~provided~~ **for example, where necessary by providing** appropriate **transparency** ~~notice~~ **notices** to data subjects, ~~obtained~~ **obtaining** necessary consents ~~, or established a legal basis for~~ **or where** ~~the transfer and processing of~~ the data ~~by~~ **is not lawfully made available to** us **. In addition** , ~~or if~~ there ~~are~~ **may be** restrictions in their terms of use of which we are not aware. In addition to data privacy and security laws, our contractual obligations relating to data privacy and security have become increasingly stringent due to changes in data privacy and security and the expansion of our service offerings. For example, certain data privacy and security laws, such as the GDPR and the CCPA, require us to impose specific contractual restrictions on our service providers **, and our customers are requiring broader and more extensive commitments**. Moreover, we ~~are~~ **have been** certified or assessed to be compliant with **certain privacy** ~~UK Cyberessentials, System~~ and **security** ~~Organization Controls (" SOC ") 1, SOC 2, SOC 3, ISO 27001, PCI- DSS 3. 2, HIPAA (under Statements on Standards~~ **standards** ~~for~~ **or requirements** ~~Attestation Engagements (" SSAE ") 21 reporting), and maintain a Federal Risk and Authorizations Management Program (" FedRAMP ") LI- SaaS Authority to Operate (" ATO ")~~. If we are unable to maintain these certifications or meet these standards, it could adversely affect our ability to provide our solutions to certain customers and could harm our business. Furthermore, we make numerous statements in our privacy policies ~~and ,~~ terms of service **, contracts, requests for information, whitepapers, in online collateral** , through our certifications to certain industry standards **,** and in our marketing materials that describe the security and privacy practices ~~of~~ **including as it relates to** our Unified- CXM platform ~~, including detailed descriptions of security measures we employ~~. Although we endeavor to comply with our public statements and documentation, we may at times fail to do so or be alleged to have failed to do so. Our privacy policies and other statements regarding data privacy and security can subject us to potential government or legal action if they are found to be deceptive, unfair **, misleading** , or misrepresentative of our actual practices. Should any of these statements prove to be untrue or be perceived as untrue, even though circumstances beyond our reasonable control, we may face litigation, disputes, claims, investigations, inquiries or other proceedings including, without limitation, by the U. S. Federal Trade Commission, federal, state and foreign regulators, our customers and private litigants, which could adversely affect our business, reputation, results of operations and financial condition. Business partners and other third parties with a strong influence on how consumers interact with our products, such as Apple, Google, Meta, Microsoft ~~,~~ and Mozilla, **have and** may **continue to** create new privacy controls or restrictions on their products and platforms, limiting the effectiveness of our services. With obligations relating to data privacy and security changing and imposing new and stringent obligations, and with some uncertainty over the interpretation and application of these and other obligations, we may face challenges in addressing their requirements and making necessary changes to our policies and practices ~~,~~ and may incur significant costs and expenses in an effort to do so. ~~Additionally, if~~ **Even with processes designed to assess** the third parties **with whom we work, we may not have sufficient knowledge about the locations where such third parties process personal data, the types of data transfers in scope for their processing, how that data is processed, or what data is processed, which may impact the commitments we can make to our customers. Additionally, if the third parties with whom** we work with, including our vendors or third- party service providers, violate applicable laws, rules or regulations or our policies, such violations ~~also~~ may put our or our customers' data at risk and could in turn have an adverse effect on our business. Any failure or perceived failure by us or ~~our~~ **the** third ~~party partners~~ **parties with whom we work** to comply with our data privacy or security obligations to customers or other third parties, or any of our other legal obligations relating to data privacy or security, may result in governmental investigations or inquiries (which have occurred in the past and may occur in the future), enforcement actions, litigation and mass arbitration demands, disputes or other claims, indemnification requests, restrictions on providing our services, claims or public statements against us by privacy advocacy groups or others, adverse press and widespread negative publicity, reputational damage, significant liability or fines and the loss of the trust of our customers, any of which could have a material adverse effect on our business, results of operations and financial condition. ~~In particular, plaintiffs have become increasingly more active in bringing privacy- related claims against companies, including class claims and mass arbitration demands. Some of these claims allow for the recovery of statutory damages on a per violation basis, and, if viable, carry the potential for monumental statutory damages, depending on the volume of data and the number of violations.~~ The cost of compliance with, and other burdens imposed by,

laws, rules, regulations and other obligations relating to data privacy and security applicable to the businesses of our customers may adversely affect our customers' ability and willingness to process personal data from their employees, customers and partners, which could limit the use, effectiveness and adoption of our Unified- CXM platform and reduce overall demand. Furthermore, the uncertain and shifting regulatory environment, as well as changes in consumer expectations concerning data privacy may cause concerns regarding data privacy and may cause our data vendors, customers or our customers' customers to resist providing the data necessary to allow our customers to use our services effectively. Even the perception of privacy concerns, whether or not valid, may inhibit market adoption, effectiveness or use of our applications. In the ordinary course of our business, we process confidential information. Use of our Unified- CXM platform also involves processing our customers' information, including personal data regarding their customers, employees or other individuals. Cyberattacks, malicious internet-based activity ~~,~~ online and offline **,** fraud **, security issues** and other similar activities threaten the confidentiality, integrity and availability of our confidential information, are prevalent and continue to increase in frequency, intensity and sophistication. Further, these threats are becoming increasingly difficult to detect and come from a variety of sources, including traditional computer " hackers, " threat actors, " hacktivists, " organized crime threat actors, personnel (such as through theft or misuse), sophisticated nation- states, and nation- state- supported actors. **In addition, our Unified- CXM platform or other internal systems used for operating our business may be misconfigured or contain significant unmitigated weaknesses or vulnerabilities, resulting in a heightened exposure to internal and external threats. The processes used to implement technical and administrative controls to protect our systems and the data they contain may be ineffective, either in parts or entirely. Our employees, contractors, partners, vendors and customers could create situations whereby critical controls are bypassed, deactivated or otherwise reduced in effectiveness, which could lead to the inadvertent exposure of confidential information, intellectual property or other sensitive information and heighten our exposure to security threats. Moreover, we may not have access to any effective control mechanisms that could mitigate these concerns or address new or advanced concerns. In the event that such weaknesses or vulnerabilities were exploited by internal or external threats, we could face adverse consequences, such as significant interruptions in our operations, loss of customers, loss of data and income, reputational harm, and diversion of funds.** Some actors now engage and are expected to continue to engage in cyber- attacks, including, without limitation, nation- state actors for geopolitical reasons and in conjunction with military conflicts and defense activities. During times of war and other major conflicts, we, the third parties ~~upon which~~ **with whom** we ~~rely~~ **work** , and our customers may be vulnerable to a heightened risk of these attacks, including retaliatory cyber- attacks, that could materially disrupt our systems and operations, supply chain, and ability to produce, sell and distribute our goods and services. We and the third parties ~~upon which~~ **with whom** we **work are** ~~rely may be~~ subject to a variety of evolving threats, including, but not limited to, social- engineering attacks (including through deep fakes, which may be increasingly more difficult to identify as fake, and phishing attacks), malicious code (such as viruses ~~and~~ **,** worms **, backdoors and time bombs**), malware (including as a result of advanced persistent threat intrusions), volumetric or application- level denial- of- service attacks, credential stuffing attacks, credential harvesting, personnel misconduct or error, ransomware attacks, supply- chain attacks, software bugs, server malfunctions, misconfiguration, software or hardware failures, access deprovisioning failures, loss of data or other information technology assets, attacks enhanced or facilitated by AI **and other similar threats** . In particular, ransomware attacks, including by organized criminal threat actors, nation- states, and nation-state- supported actors, are prevalent and severe and can lead to significant interruptions in our operations, loss of data and income, reputational harm, and diversion of funds. Extortion payments may alleviate the negative impact of a ransomware attack, but we may be unwilling or unable to make such payments due to, for example, applicable laws or regulations prohibiting such payments. Adware, telecommunications failures, earthquakes, fires, floods, adverse weather events, and man- made disasters may also impact the availability of our systems and operations. **Additionally, our customers have in the past conducted, and may continue to conduct in the future, their own penetration testing on our systems, potentially uncovering issues or vulnerabilities. The discovery of vulnerabilities in our systems by customers could result in adverse consequences, including contractual penalties, customer churn and reputational damage.** Furthermore, our services are ~~critical~~ **important** to the internal processes of **many** ~~a large number~~ of ~~companies~~ **our customers** worldwide and, as a result, if our products are compromised, a significant number or, in some instances, all of our customers and their data could be simultaneously affected, which could cause serious disruption and harm. The potential liability and associated consequences we could suffer as a result could be significant. Our remote workforce poses increased risks to our information technology systems and data, as more of our employees utilize network connections, computers, and devices outside our premises or network, including while working from home, while in transit, and in public locations. Future or past business transactions (such as acquisitions or integrations) could expose us to additional cybersecurity risks and vulnerabilities, as our systems could be negatively affected by vulnerabilities present in acquired or integrated entities' systems and technologies. We may also discover security issues that were not identified during due diligence of such acquired or integrated entities, and it may be difficult to integrate other companies into our information technology environment and security program. We rely upon third parties and third- party technologies to operate critical business systems to process confidential information in a variety of contexts, including, without limitation, third- party providers of cloud- based infrastructure, encryption and authentication technology, employee email, content delivery to customers, and other functions. While we require the third parties ~~upon which~~ **with whom** we ~~rely~~ **work** to process confidential information on our behalf to meet certain security requirements and give contractual commitments to us regarding their data processing activities, our ability to monitor these third parties' information security practices is limited, and despite such assurance and commitments, these third parties may not have, or may not continue to have, adequate information security measures in place. If the third parties ~~upon which~~ **with whom** we ~~rely~~ **work** experience a security incident or other interruption, we could experience adverse consequences. While we may be entitled to damages if these third parties fail to satisfy their privacy or security- related obligations to us, any award may be insufficient to cover our damages or

protect our reputation, or we may be unable to recover any such awarded damages. Moreover, supply- chain attacks have increased in frequency and severity, and we cannot guarantee that third parties and infrastructure in our supply chain or in the third parties' ~~upon which~~ **with whom** we ~~rely~~ **work** supply chains have not been compromised or that they do not contain exploitable vulnerabilities, defects or bugs that could result in a breach of or disruption to our information technology systems (including our products and services) or the third- party information technology systems that support us and our services. Additionally, the reliability and continuous availability of our platform **and services** is critical to our success. We take steps designed to detect, mitigate, and remediate vulnerabilities in our information systems (such as our hardware, software, and products, and those of the third parties ~~upon which~~ **with whom** we ~~rely~~ **work**). However, our information systems may contain errors, defects, security vulnerabilities, or software bugs that are difficult to detect and correct, and some of these may pose a significant risk to our business and ability to provide our products and services, particularly when such vulnerabilities are first introduced or when new versions or enhancements of our platform are released. We have not always been able in the past and may be unable in the future to detect and remediate all such vulnerabilities in our information systems including on a timely basis **, and sometimes customer permission to remediate certain vulnerabilities may be required, which could result in further delays in timely remediation** . Despite our efforts to identify and remediate vulnerabilities and related unauthorized access in our information technology systems (including our products), our efforts may not be successful. Further, in some cases, these vulnerabilities may require immediate attention, but we may still experience delays in developing and deploying remedial measures designed to address any such vulnerabilities. Even if we have issued or otherwise made patches or information for vulnerabilities in our information systems, our customers may be unwilling or unable to deploy such patches and use such information effectively and in a timely manner. Vulnerabilities could be exploited and result in a security incident. ~~Any~~ **Certain** of the previously identified or similar threats ~~could~~ **have in the past and may in the future** cause a security incident or other interruption that could result in unauthorized, unlawful, or accidental acquisition, modification, destruction, loss, alteration, encryption, disclosure of, or access to our confidential information. A security incident or other interruption could disrupt our ability (and that of third parties ~~upon which~~ **with whom** we ~~rely~~ **work**) to provide our Unified- CXM platform and our services **, lead to the termination of our contracts by our customers and / or vendors and monetary penalties based on our agreements with said customers and / or vendors** . We may expend significant resources or modify our business activities to try to **remediate and** protect against security incidents. While we have implemented security measures designed to protect against security incidents, there can be no assurance that these measures will be effective. We have in the past and may in the future be subject to attempted or successful cybersecurity attacks by third parties seeking unauthorized access to our or our customers' confidential information or to disrupt our ability to provide our Unified- CXM platform. Our data privacy and security obligations under **certain** applicable laws and our customer agreements ~~may~~ require us to implement and maintain specific security measures, industry- standard or reasonable security measures to protect our information technology systems and confidential information. ~~We~~ **At times, we may fail, or be perceived to have failed, in implementing these privacy and security obligations. Such actual or perceived non- compliance by us or the third parties with whom we work could result in adverse consequences. In addition, we** operate our products for the benefit of our customers who have documented responsibilities to maintain certain security controls, such as provisioning and deprovisioning users, in their respective environments without oversight or control by us. Our customers **are responsible for using, configuring and otherwise implementing security measures related to our platform, services and products in a manner that meets applicable cybersecurity standards, complies with laws, and addresses their information security risk. In certain cases, our customers** may **reject,** weaken or incorrectly configure security controls provided by us to maintain the security of their environments, resulting in a loss of confidentiality or integrity of such customer' s data or processes. Such an event also may result in a compromise to our information technology systems or a security incident, or public disclosures and negative publicity for us and such customer, which may have a negative impact on our ability to achieve our corporate goals and could adversely affect our business, reputation, results of operations and financial condition. Such an event may also result in a compromise to our information technology systems or a security incident. Applicable data privacy and security obligations, both legally and contractually, may require us **, or we may choose,** to notify relevant stakeholders **, including affected individuals, customers, regulators, and investors,** of security incidents **, or to take other actions, such as providing credit monitoring and identity theft protection services** . Such notifications are costly, and the notifications or the failure to comply with such requirements could lead to adverse consequences **, including breach of contract or applicable legislation** . If we (or a third party ~~upon which~~ **with whom** we ~~rely~~ **work**) experience a security incident or are perceived to have experienced a security incident, we may experience adverse consequences. These consequences may include: government enforcement actions (for example, investigations, fines, penalties, audits, and inspections) **; regulatory investigations or requests for information** ; additional reporting requirements and / or oversight; restrictions on processing confidential information (including personal data); litigation (including class claims); indemnification obligations; negative publicity; reputational harm; monetary fund diversions; interruptions in our operations (including availability of data); financial loss; and other similar harms. Security incidents and attendant consequences may prevent or cause customers to stop using our Unified- CXM platform, deter new customers from using our Unified- CXM platform, and negatively impact our ability to grow and operate our business. **Additionally, we may make statements that describe our efforts to respond to, mitigate and / or remediate security incidents. Although we endeavor to be as accurate as possible in our statements, we may at times fail to do so or be alleged to have failed to do so. Our statements related to our response to security incidents can subject us to potential government or legal action if they are found to be deceptive, misleading, or misrepresentative of our actual practices. Should any of these statements prove to be untrue or be perceived as untrue, we may face litigation, disputes, claims, investigations, inquiries or other proceedings including, without limitation, by the U. S. Federal Trade Commission and federal, state and foreign regulators, which could adversely affect our business, reputation, results of operations and financial condition.** Our

contracts may not contain limitations of liability, and even where they do, there can be no assurance that limitations of liability in our contracts are sufficient to protect us from liabilities, damages, or claims related to our data privacy and security obligations. We cannot be sure that our insurance coverage will be adequate or sufficient to protect us from or to mitigate liabilities arising out of our privacy and security practices, that such coverage will continue to be available on commercially reasonable terms or at all, or that such coverage will pay future claims. In addition to experiencing a security incident, third parties may gather, collect, or infer sensitive information about us from public sources, data brokers, or other means that reveals competitively sensitive details about our organization and could be used to undermine our competitive advantage or market position. Risks Related to Tax and Accounting Matters Our results of operations may be harmed if we are required to collect sales, value- added, goods and services or other similar taxes for subscriptions to our products and services in jurisdictions in which we have not historically done so. Sales tax, value- added tax (" VAT "), goods and services tax (" GST "), and other similar transaction tax laws and rates differ greatly by jurisdiction and are subject to varying interpretations that may change over time. The application of these tax laws to services provided electronically is evolving. In particular, the applicability of sales taxes to our products and services in various jurisdictions is unclear. Furthermore, an increasing number of states have considered or adopted laws that attempt to impose tax collection obligations on out- of- state companies. The Supreme Court of the United States ruled in South Dakota v. Wayfair, Inc. et al (" Wayfair "), that online sellers can be required to collect sales and use tax despite not having a physical presence in the buyer' s state or " economic nexus. " In response to Wayfair, or for other reasons, states or local governments have adopted and begun to enforce, and other states or local governments may adopt, or begin to enforce, laws requiring us to calculate, collect, and remit taxes on sales in their jurisdictions. Similarly, many non- U. S. jurisdictions have considered or adopted laws that impose VAT, digital service, or similar taxes, on companies despite not having a physical presence in the non- U. S. jurisdiction. We collect sales tax, VAT or similar transaction taxes in a number of jurisdictions. It is possible, however, that we could face sales tax, VAT, GST or similar tax audits and that our liability for these taxes could exceed our estimates if state, local, and non- U. S. tax authorities assert that we are obligated to collect additional tax amounts from our customers and remit those taxes to those authorities. We also could be subject to audits in state, local and non- U. S. jurisdictions for which we have not accrued tax liabilities. A successful assertion by one or more states, localities or non- U. S. jurisdictions requiring us to collect taxes where we presently do not do so, or to collect more taxes in a jurisdiction in which we currently do collect some taxes, could result in substantial tax liabilities, including taxes on past sales, as well as penalties and interest. Such tax assessments, penalties, and interest, or future requirements may adversely affect our results of operations. Our international operations subject us to potentially adverse tax consequences. We generally conduct our international operations through subsidiaries and are subject to income taxes as well as non- income- based taxes, such as payroll, value- added, goods and services and other local taxes in various jurisdictions. Our domestic and international tax liabilities are subject to rules regarding the calculation of 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 relevant taxing authorities may disagree with our determinations as to the value of assets sold or acquired or the income and expenses attributable to specific jurisdictions. If such a disagreement were to occur and our position were 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. Changes in, or interpretations of, tax rules and regulations may adversely affect our effective tax rates. Changes in tax law (including tax rates) could affect our future results of operations. Due to the expansion of our international business activity, any such changes could increase our worldwide effective tax rate and adversely affect our business, results of operations and financial condition. For example, recent legislation in the United States, commonly referred to as the Inflation Reduction Act, enacts a minimum tax equal to 15 percent of the adjusted financial statement income of certain large U. S. corporations, as well as a one percent excise tax on stock repurchases imposed on public corporations making such repurchases. It is possible that the Inflation Reduction Act could increase our tax liability. The current or future U. S. presidential administration could propose or enact changes to U. S. tax laws that we cannot currently predict and that could materially affect our business, results of operations and financial condition. Additionally, the Organization for Economic Co- operation and Development (" OECD ") has released guidance covering various topics, including transfer pricing, country- by- country reporting and definitional changes to permanent establishment that could ultimately impact our tax liabilities as countries adopt the OECD' s guidance. **The OECD Pillar 2 guidelines address the increasing digitalization of the global economy and re-allocating taxing rights among countries. The European Union and many other member states have committed to adopting Pillar 2, which calls for a global minimum tax of 15 % to be effective for tax years beginning in 2024. The OECD guidelines published to date include transition and safe harbor rules around the implementation of the Pillar 2 global minimum tax. We are monitoring developments and evaluating the impacts these new rules will have on our tax rate, including eligibility to qualify for these safe harbor rules.** We are subject to tax examinations of our tax returns by the Internal Revenue Service (the " IRS "), and other domestic and foreign tax authorities. An adverse outcome of any such audit or examination by the IRS or other tax authority could have a material adverse effect on our results of operations and financial condition. We are, and expect to continue to be, subject to audit by the IRS and other tax authorities in various domestic and foreign jurisdictions. As a result, we have received, and may in the future receive, assessments in multiple jurisdictions on various tax- related matters. Taxing authorities also have challenged, and may in the future challenge, our tax positions and methodologies on various matters. We regularly assess the likelihood of adverse outcomes resulting from ongoing tax examinations to determine the adequacy of our provision for income taxes. These assessments can require considerable estimates and judgments. The calculation of our tax liabilities involves uncertainties in the application of complex tax laws and regulations in a variety of jurisdictions. There can be no assurance that our tax positions and methodologies are accurate or that the outcomes of ongoing and future tax examinations will not have an adverse effect on our results of operations and financial

condition. Our ability to use our net operating losses and other tax assets to offset future taxable income or tax liability **could** be subject to certain limitations. We have U. S. federal and state net operating loss (" NOL ") carryforwards as a result of prior period losses, some of which, if not utilized, may expire. Certain of our federal NOLs will begin to expire in fiscal year 2032 and our state NOLs began to expire in fiscal year 2023. If these net operating loss carryforwards expire unused, they will be unavailable to offset future income tax liabilities, which could adversely affect our potential profitability. **U. S. federal NOLs incurred in taxable years beginning after December 31, 2017 may be carried forward indefinitely, but such federal NOL carryforwards are permitted to be used in any taxable year to offset only up to 80 % of taxable income in such year. U. S. federal NOLs incurred in taxable years beginning after December 31, 2017 generally are not permitted to be carried back to prior taxable years.** In addition, under Section 382 of the Internal Revenue Code of 1986, as amended (the " Code "), **our ability to utilize net operating loss carryforwards in any taxable year may be limited** if **we experience** ~~a corporation undergoes~~ an " ownership change ~~,~~**.** " **An** ~~its ability to use its pre- change net operating loss carryforwards and other tax attributes to offset its post- change taxable income or tax liability may be limited. Such an~~ " ownership change " generally occurs if ~~there is a greater than 50 percentage point change (by value) in our equity ownership by~~ one or more stockholders or groups of stockholders who own at least 5 % of our stock **increase their ownership by more than 50 percentage points** over **their lowest ownership percentage within** a **rolling** three- year period. ~~We~~ **Similar rules may apply under state tax laws. Future issuances of our stock could cause an " ownership change. " It is possible that any future ownership change could** have ~~experienced ownership changes in the past and may experience ownership changes in the future as~~ a **material effect on the** ~~result of subsequent shifts in our stock ownership. As a result, if we earn net taxable income, our ability to~~ use **of** our ~~pre- change~~ net operating loss carryforwards ~~and other pre- change tax attributes to offset U. S. federal and state taxable income or tax liability may be subject to limitations~~, which could **adversely affect our profitability** ~~potentially result in increased future tax liability to us~~. ~~Furthermore~~ **In addition** , ~~under~~ **at the state level,** ~~the~~ **there may be periods during which** ~~current U. S. federal tax laws,~~ the ~~amount of net operating loss carryforwards from tax years beginning after December 31, 2017 that we are permitted to~~ use **of NOLs** ~~in any taxable year~~ is **suspended or otherwise** limited **which** ~~to 80 % of our taxable income in such year, where taxable income is determined without regard to the net operating loss deduction itself. Under current U. S. federal tax laws, net operating losses generally are not permitted to be carried back to prior taxable years. There is also a risk that, due to regulatory changes, such as suspensions of the use of NOLs, or other unforeseen reasons, our existing NOLs~~ could **accelerate** ~~expire or otherwise be unavailable to offset future income tax liabilities. For~~ **or permanently increase state** ~~these reasons, we may not be able to realize a tax~~ **taxes owed** ~~benefit from the use of our NOLs, whether or not we attain profitability~~. Risks Related to Being a Public Company, Ownership of Our Class A Common Stock and Other General Risks The market price of our Class A common stock may fluctuate or decline substantially depending 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, including: • price and volume fluctuations in the overall stock market from time to time **, including as a result of any future share repurchase program implemented by the company** ; • announcements of new products, solutions or technologies, commercial relationships, acquisitions or other events by us or our competitors; • changes in how enterprises perceive the benefits of our Unified- CXM platform and products; • departures of key personnel; • the public' s reaction to our press releases, other public announcements and filings with the SEC; • fluctuations in the trading volume of our shares or the size of our public float; • sales of large blocks of our common stock; • market manipulation, including coordinated buying or selling activities; • actual or anticipated changes or fluctuations in our results of operations; • whether our results of operations meet the expectations of securities analysts or investors; • changes in actual or future expectations of investors or securities analysts; • actual or perceived significant data breach involving our Unified- CXM platform; • **our involvement in any** litigation ~~involving us~~, ~~our industry or both~~ **including class action lawsuits** ; • governmental or regulatory actions or audits; • regulatory **or political** developments in the United States, foreign countries or both **, including potential implications from the recent elections in the United States** ; • general economic, political and market conditions and overall fluctuations in the financial markets in the United States and abroad, including as a result of ~~recent bank closures,~~ public health crises or geographical tensions and wars, such as the Russia- Ukraine war and the Israel- Hamas war (including any escalation or ~~geographical~~ **geopolitical** expansion of these conflicts); and • " flash crashes, " " freeze flashes " or other glitches that disrupt trading on the securities exchange on which we are listed. The market for technology stocks and the stock market in general have recently experienced significant price and volume fluctuations that have affected and continue to affect the market prices of equity securities of many companies, including our own. These fluctuations have often been unrelated or disproportionate to the operating performance of these companies. Broad market and industry fluctuations, as well as general economic, political, regulatory and market conditions, may continue to negatively impact investor confidence and the market price of equity securities, including our Class A common stock ~~. In the past, following periods of volatility in the trading price of a company' s securities, securities class action litigation has often been brought against that company. If the market price of our Class A common stock is volatile, we may become the target of securities litigation. Securities litigation 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~~. The dual class structure of our common stock as contained in our amended and restated certificate of incorporation has the effect of concentrating voting control with our executive officers and directors and their affiliates, limiting your ability to influence corporate matters. Our Class B common stock has ten votes per share, and our Class A common stock has one vote per share. The holders of our Class B common stock as of January 31, ~~2024~~ **2025** beneficially held approximately ~~44~~ **45** . ~~6~~ **5** % of our outstanding capital stock, but controlled approximately 89. ~~0~~ **3** % of the voting power of our outstanding capital stock. Therefore, the holders of Class B common stock have control over our management and affairs and over all matters requiring stockholder approval, including election of directors and significant corporate transactions, such as a merger or other sale of us or our assets, for the foreseeable future. In addition, the holders of

Class B common stock collectively will continue to be able to control all matters submitted to our stockholders for approval even if their stock holdings represent less than a majority of the outstanding shares of our common stock. This concentrated control will limit your ability to influence corporate matters for the foreseeable future, and, as a result, the market price of our Class A common stock could be adversely affected. As of January 31, ~~2024~~ **2025**, our directors, executive officers and their respective affiliates beneficially owned, in the aggregate, approximately 98. ~~0~~ **3** % of our Class B common stock, and controlled approximately ~~88~~ **89**. ~~8~~ **7** % of the voting power of our outstanding capital stock. As a result, our directors, executive officers and their respective affiliates, if acting together, are able to determine or significantly influence all matters requiring stockholder approval, including the elections of directors, amendments of our organizational documents and approval of any merger, sale of assets or other major corporate transaction. These stockholders may 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 will limit the ability of other stockholders to influence corporate matters and may cause us to make strategic decisions that could involve risk to holders of our Class A common stock or that may not be aligned to the interest of holders of our Class A common stock, including decisions to delay, prevent or discourage acquisition proposals or other offers for our capital stock that you may feel are in your best interest as a stockholder and ultimately could deprive you of an opportunity to receive a premium for your Class A common stock as part of a sale of our company, which in turn might adversely affect the market price of our common stock. ~~We cannot guarantee that our share repurchase program will be fully consummated or that it will enhance long- term stockholder value. Share repurchases could also increase the volatility of the trading price of our common stock and could diminish our cash reserves. Our board of directors has approved a share repurchase program to repurchase up to $ 200 million of our Class A common stock through December 31, 2024 in open market purchases at prevailing market prices or in negotiated transactions off the market, including, without limitation, accelerated share repurchase transactions, collared accelerated share repurchase transactions, volume weighted average purchase prepaid forward transactions and similar arrangements (the " 2024 repurchase program "). Although our board of directors has authorized the 2024 repurchase program, it does not obligate us to repurchase any specific dollar amount or to acquire any specific number of shares. The actual timing, manner, price and total amount of future repurchases will depend on a variety of factors, including business, economic and market conditions, corporate and regulatory requirements, prevailing stock prices, restrictions under the terms of loan agreements and other considerations. The 2024 repurchase program may be modified, suspended, or terminated at any time, and we cannot guarantee that the program will be fully consummated or that it will enhance long- term stockholder value. The 2024 repurchase program could affect the trading price of our stock and increase volatility, and any announcement of a termination of this program may result in a decrease in the trading price of our stock. In addition, the 2024 repurchase program could diminish our cash and cash equivalents and marketable securities.~~ If we fail to maintain an effective system of disclosure controls and internal control over financial reporting, our ability to produce timely and accurate financial statements or comply with applicable regulations could be impaired. As a public company, we are subject to the reporting requirements of the Exchange Act, the Sarbanes- Oxley Act, and the listing standards of the New York Stock Exchange. The Sarbanes- Oxley Act requires, among other things, that we maintain effective disclosure controls and procedures and internal control over financial reporting. We have expended, and anticipate that we will continue to expend, significant resources in order to maintain and improve the effectiveness of our disclosure controls and procedures and internal control over financial reporting. In addition, pursuant to Section 404 of the Sarbanes Oxley- Act, we are required to perform system and process evaluation and testing of our internal control over financial reporting to allow our management to furnish a report on, among other things, the effectiveness of our internal control over financial reporting, and we are also required to have our independent registered public accounting firm issue an opinion on the effectiveness of our internal control over financial reporting on an annual basis. Our current controls and any new controls that we develop may become inadequate because of changes in the conditions in our business, including increased complexity resulting from our international expansion. Further, weaknesses in our disclosure controls or our internal control over financial reporting have been and may be discovered in the future. Any failure to develop or maintain effective controls, or any difficulties encountered in their implementation or improvement, could harm our results of operations or cause us to fail to meet our reporting obligations and may result in a restatement of our financial statements for prior periods. Any failure to implement and maintain effective internal control over financial reporting also could adversely affect the results of periodic management evaluations and annual independent registered public accounting firm attestation reports regarding the effectiveness of our internal control over financial reporting that we will eventually be required to include in our periodic reports that will be filed with the SEC. Ineffective disclosure controls and procedures and internal control over financial reporting also could cause investors to lose confidence in our reported financial and other information, which would likely adversely affect the market price of our Class A common stock. In addition, if we are unable to continue to meet these requirements, we may not be able to remain listed on the New York Stock Exchange. If we are unable to assert that our internal control over financial reporting is effective, or if our independent registered public accounting firm is unable to express an opinion on the effectiveness of our internal control over financial reporting, investors could lose confidence in the reliability of our financial statements, the market price of our common shares could decline and we could be subject to sanctions or investigations by the New York Stock Exchange, the SEC or other regulatory authorities. Any failure to maintain effective disclosure controls and internal control over financial reporting could have an adverse effect on our business, results of operations and financial condition and could cause a decline in the market price of our Class A common stock. **Our business depends to a significant extent on the overall demand for enterprise cloud software products and on the economic health of our current and prospective customers.** The global economy, including credit and financial markets, has experienced extreme volatility and disruptions, including severely diminished liquidity and credit availability, declines in consumer confidence, declines in economic growth, increases in unemployment rates, ~~increases~~ **fluctuations** in inflation **and** ~~rates, higher~~ interest rates, disruptions in access to bank deposits or lending commitments due to bank failures and uncertainty about economic stability. **The** ~~For example, the COVID- 19~~

~~pandemic resulted in widespread unemployment, economic slowdown and extreme volatility in the capital markets. Similarly, the~~ Russia- Ukraine war has also added to, and the Israel- Hamas war and related regional tensions may add to, the extreme volatility in the global capital markets and is expected to have further global economic consequences, including disruptions of the global supply chain and energy markets. In addition, ~~rising~~ **fluctuations in** inflation and other macroeconomic pressures in the U. S. and the global economy could exacerbate extreme volatility in the global capital markets and heighten unstable market conditions. Any such volatility and disruptions may have adverse consequences on us or the third parties on whom we rely. If the equity and credit markets continue to deteriorate, including as a result of ~~recent~~ bank closures, public health crises, or political unrest, war or a global or domestic recession or the fear thereof, it may make any necessary debt or equity financing more difficult to obtain in a timely manner or on favorable terms, more costly or more dilutive. Increased inflation rates can adversely affect us by increasing our costs, including labor and employee benefit costs. In addition, higher inflation also could increase our customers' operating costs, which could result in reduced marketing budgets for our customers and potentially less demand for our platform. Any significant increases in inflation and related increase in interest rates could have a material adverse effect on our business, results of operations and financial condition. To the extent that these weak economic conditions cause our existing customers or potential customers to reduce their budget for Unified- CXM solutions or to perceive spending on such systems as discretionary, demand for our Unified- CXM platform may be adversely affected. Moreover, **general economic weakness may lead to longer collection cycles for payments due from our customers, an increase in customer bad debt and restructuring initiatives and associated expenses, and** customers and potential customers may require ~~extended billing terms and other~~ financial concessions, **all of** which would limit our ability to grow our business and adversely affect our business, results of operations and financial condition. In the event of a catastrophic event, including a natural disaster such as an earthquake, hurricane, fire, flood, tsunami or tornado, or other catastrophic event such as power loss, market manipulation, civil unrest, supply chain disruptions, armed conflict, computer or telecommunications failure, cybersecurity issues, human error, improper operation, unauthorized entry, break- ins, sabotage, intentional acts of vandalism and similar misconduct, war, terrorist attack or incident of mass violence in any geography where our operations or data centers are located or where certain other systems and applications that we rely on are hosted, we may be unable to continue our operations and may endure significant system degradations, disruptions, destruction of critical assets, reputational harm, delays in our application development, breaches of data security and loss of critical data, all of which could have an adverse effect on our future results of operations. We also rely on our employees and key personnel to meet the demands of our customers and run our day- to- day operations. In the event of a catastrophic event, the functionality of our employees could be negatively impacted, which could have an adverse effect on our business, financial condition and results of operations. In addition, natural disasters, cybersecurity attacks, market manipulations, supply chain disruptions, acts of terrorism or other catastrophic events could cause disruptions in our or our customers' businesses, national economies or the world economy as a whole. Delaware law and provisions in our amended and restated certificate of incorporation and amended and restated bylaws could make a merger, tender offer or proxy contest difficult, thereby depressing the market price of our Class A common stock. Our status as a Delaware corporation and the anti- takeover provisions of the Delaware General Corporation Law may discourage, delay or prevent a change in control by prohibiting us from engaging in a business combination with an interested stockholder for a period of three years after the date of the transaction in which the person became an interested stockholder, even if a change of control would be beneficial to our existing stockholders. In addition, our amended and restated certificate of incorporation and amended and restated bylaws contain provisions that may make the acquisition of our company more difficult, including the following: • vacancies on our board of directors may be filled only by our board of directors and not by stockholders; • our board of directors is classified into three classes of directors with staggered three- year terms; • our stockholders may only take action at a meeting of stockholders and may not take action by written consent for any matter; • a special meeting of our stockholders may only be called by a majority of our board of directors, the chairperson of our board of directors or our Chief Executive Officer; • advance notice procedures apply for stockholders to nominate candidates for election as directors or to bring matters before an annual meeting of stockholders; • our amended and restated certificate of incorporation does not provide for cumulative voting; • our amended and restated certificate of incorporation will allow stockholders to remove directors only for cause; • certain amendments to our amended and restated certificate of incorporation will require the approval of the holders of at least 66 2 / 3 % of our then- outstanding common stock; • authorize undesignated preferred stock, the terms of which may be established and shares of which may be issued by our board of directors, without further action by our stockholders; and • certain litigation against us can only be brought in Delaware. These provisions, alone or together, could discourage, delay or prevent a transaction involving a change in control of our company. These provisions also could discourage proxy contests and make it more difficult for stockholders to elect directors of their choosing and to cause us to take other corporate actions they desire, any of which, under certain circumstances, could limit the opportunity for our stockholders to receive a premium for their shares of our capital stock, and also could affect the price that some investors are willing to pay for our Class A common stock. Our charter documents designate a state or federal court located within the State of Delaware as the exclusive forum for substantially all disputes between us and our stockholders, and also provide that the federal district courts are the exclusive forum for claims under the Securities Act, which could limit our stockholders' ability to choose the judicial forum for disputes with us or our directors, officers or employees. Our amended and restated bylaws provide that, unless we consent in writing to the selection of an alternative forum, to the fullest extent permitted by law, the sole and exclusive forum for the following types of actions and proceedings under Delaware statutory or common law: (i) any derivative action or proceeding brought on our behalf; (ii) any action asserting a claim of breach of a fiduciary duty owed by any of our directors, officers or other employees to us or our stockholders; (iii) any action arising pursuant to any provision of the Delaware General Corporation Law, our amended and restated certificate of incorporation or our amended and restated bylaws or (iv) any other action asserting a claim that is governed by the internal affairs doctrine shall be the Court of Chancery of the State of Delaware (or, if the Court of Chancery

does not have jurisdiction, the federal district court for the District of Delaware), in all cases subject to the court having jurisdiction over indispensable parties named as defendants. This exclusive forum provision will not apply to any causes of action arising under the Securities Act or the Exchange Act or any other claim for which the federal courts have exclusive jurisdiction. In addition, our amended and restated certificate of incorporation provides that, unless we consent in writing to the selection of an alternative forum, to the fullest extent permitted by law, the federal district courts of the United States of America shall be the exclusive forum for the resolution of any complaint asserting a cause of action arising under the Securities Act. This provision is intended to benefit and may be enforced by us, our officers and directors, the underwriters to any offering giving rise to such complaint, and any other professional entity whose profession gives authority to a statement made by that person or entity and who has prepared or certified any part of the documents underlying the offering. Any person or entity purchasing or otherwise acquiring any interest in any of our securities shall be deemed to have notice of and consented to this provision. This exclusive- forum provision may limit a stockholder' s ability to bring a claim in a judicial forum of its choosing for disputes with us or our directors, officers or other employees, which may discourage lawsuits against us and our directors, officers and other employees. If a court were to find the exclusive- forum provision in our charter documents to be inapplicable or unenforceable in an action, we may incur additional costs associated with resolving the dispute in other jurisdictions, which could harm our results of operations.