Risk Factors Comparison 2025-01-21 to 2024-01-26 Form: 10-K

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

We operate in a rapidly changing environment that involves certain risks and uncertainties, some of which are beyond our control. The risks discussed below could materially affect our business, financial condition and future results. The risks described below are not the only risks we face. Additional risks and uncertainties not currently known to us or that we currently deem to be immaterial may materially adversely affect our business, financial condition or operating results in the future. Risks Related to Our Ability to Grow Our Business Technology and customer requirements evolve rapidly in our industry, and if we do not continue to develop **or acquire** new products and enhance our existing products in response to these changes, our business could be harmed. Ongoing enhancements to our product sets (both organically and through acquisitions) will be required to enable us to maintain our competitive position and the competitive position of our ISVs, distributors / resellers, and OEMs. We may not be successful in developing and marketing enhancements to our products on a timely basis, and any enhancements we develop may not adequately address the changing needs of the marketplace. Overlaying the risks associated with our existing products and enhancements are ongoing technological developments and rapid changes in customer and partner requirements. Our future success will depend upon our ability to develop, acquire and introduce new products in a timely manner that take advantage of technological advances and respond to new customer and partner requirements. We may not be successful in developing or acquiring new products incorporating new technology on a timely basis, and any new products we develop or acquire may not adequately address the changing needs of the marketplace or may not be accepted by the market. Failure to develop new products and product enhancements that meet market needs in a timely manner could have a material adverse effect on our business, financial condition and operating results. We are substantially dependent on our OpenEdge products. We derive a significant portion of our revenue from software license and maintenance revenue attributable to our OpenEdge product set, which in fiscal year ~~2023~~ **2024** accounted for approximately ~~37~~ **34** % of our aggregate revenue on a consolidated basis. Accordingly, our future results depend on continued market acceptance of OpenEdge. If consumer demand declines, or new technologies emerge that are superior to, or are more responsive to customer requirements than OpenEdge, such that we are unable to maintain OpenEdge' s competitive position within its marketplace, our business, financial condition and operating results may be materially adversely affected. The segments of the software industry in which we participate are intensely competitive, and our inability to compete effectively could harm our business. We experience significant competition from a variety of sources with respect to the marketing and distribution of our products. Many of our competitors have greater financial, marketing or technical resources than we do and may be able to adapt more quickly to new or emerging technologies and changes in customer requirements or to devote greater resources to the promotion and sale of their products than we can. Increased competition could make it more difficult for us to maintain our market presence or lead to downward pricing pressure. In addition, current and potential competitors may make strategic acquisitions or establish cooperative relationships among themselves or with third parties, thereby increasing their ability to deliver products that better address the needs of our **existing or** prospective customers. Current and potential competitors may also be more successful than we are in having their products or technologies widely accepted. We may be unable to compete successfully against current and future competitors, and our failure to do so could have a material adverse effect on our business, prospects, financial condition and operating results. The value of our Chef software assets may be limited by open source development and licensing practices. Our Chef offerings incorporate software components licensed to the general public under open source licenses. We obtain many components from software developed and released by contributors to independent open source components of our offerings. One of the characteristics of open source software is that the governing license terms generally allow liberal modifications of the code and distribution to a wide group of companies and / or individuals. As a result, the marketplace for new products is intensely competitive and characterized by low barriers to entry because others could develop new software products or services based upon those open source programs that compete with existing open source software that we support and incorporate into our Chef products. New competitors ~~possessing technological, marketing or other competitive advantages~~ that develop their own open source software or hybrid proprietary and open source software offerings **with technological , marketing or other competitive advantages** may reduce the demand for ~~,~~ and ~~putting~~ **impose** price pressure on ~~,~~ our products **,** enabling them to rapidly acquire market share ~~,~~ and limit the value of our software assets. We intend to make additional acquisitions of businesses, products or technologies that involve additional risks, which could disrupt our business or harm our financial condition, results of operations or cash flows. A key element of our strategy includes the acquisition of businesses that offer complementary products, services and technologies, augment our revenues and cash flows, and meet our strict financial and other criteria. We may not be able to identify suitable acquisition opportunities or consummate any such transactions **on favorable terms or at all** . Even if an acquisition is successful, **the** integration of a new business involves a number of risks that could have a material adverse effect on our business, financial condition, operating results or cash flows, including: • difficulties of assimilating the operations and personnel, products or systems of acquired companies; • our potential inability to realize the value of the acquired assets relative to the price paid; • distraction of **our** management from our ongoing businesses; • potential product disruptions associated with the sale of the acquired business' s products; • the potential that an acquisition may not further our business strategy as we expected, may not result in revenue and cash flow growth to the degree we expected or at all, or may not achieve expected synergies; • the possibility of incurring significant restructuring charges and amortization expense; • the risk that an acquired company' s cybersecurity may not have been sufficient and could cause a post- acquisition risk once integrated into our systems; • risks related to the assumption of the acquired business' s liabilities or any ongoing lawsuits; • potential impairment to assets

that we recorded as a part of an acquisition, including intangible assets and goodwill; and • to the extent that we issue stock to pay for an acquisition, dilution to existing stockholders and decreased earnings per share. Difficulties associated with any acquisitions we may pursue, and their integration may be complicated by factors such as: • the size of the business or entity acquired; • geographic and cultural differences; • lack of experience operating in the industry or markets of the acquired business (e. g., satisfying the requirements of public- sector customers); • potential loss of key employees and customers; • the potential for deficiencies in internal controls at the acquired or combined business, including but not limited to with regard to any weaknesses or vulnerabilities in ~~a target~~ **the acquired** company' s cybersecurity controls; • performance problems with the acquired business' s technology; • exposure to unanticipated liabilities of the acquired business, including any cybersecurity issues; • insufficient revenue to offset increased expenses associated with the acquisition; and • adverse tax consequences. In addition, if we fail to complete an announced acquisition, **the market price of** our **common** stock ~~price~~ could fall to the extent ~~the~~ **such** price reflects an assumption that such acquisition will be completed, and we may incur significant unrecoverable costs. Further, the failure to consummate an acquisition may result in negative publicity and adversely impact our relationships with our customers, vendors and employees. We may become subject to legal proceedings relating to the acquisition and the integration of acquired businesses may not be successful. Failure to manage and successfully integrate acquired businesses, achieve anticipated levels of profitability of the acquired business, improve margins of the acquired businesses and products, or realize other anticipated benefits of an acquisition could materially harm our business, operating results and margins. If our goodwill or amortizable intangible assets become impaired, we may be required to record a significant charge to earnings. We acquire other companies and intangible assets and may not realize all the economic benefit from those acquisitions, which could cause an impairment of goodwill or intangibles. We review our amortizable intangible assets for impairment when events or changes in circumstances indicate the carrying value may not be recoverable. We test goodwill for impairment at least annually. Factors that may cause a change in circumstances, indicating that the carrying value of our goodwill or amortizable intangible assets may not be recoverable, include a decline in **the market price of** our **common** stock ~~price~~ and market capitalization, reduced future cash flow estimates, and slower growth rates in industry segments in which we participate. We may be required to record a significant charge in our consolidated financial statements during the period in which any impairment of our goodwill or amortizable intangible assets is determined, ~~negatively~~ **adversely** affecting our results of operations . Integration of artificial intelligence into our..... prevent or limit our use of AI . Risks Related to the Operation of Our Business ~~Our realignment initiatives may disrupt our operations and we may not achieve the expected benefits from our efforts. We have restructured or made other adjustments to our workforce in response to management changes, product changes, performance issues, changes in strategy, acquisitions and other internal and external considerations; and we may undertake similar restructuring or realignment initiatives in the future. In the past, realignment initiatives have resulted in increased restructuring costs and have temporarily reduced productivity. Future realignment initiatives may be complex and could result in significant costs and expenses, which could negatively impact our reputation, financial condition, operating results and shareholder value. There can be no assurance that we can accomplish or implement all of the desired initiatives, or that the activities under those initiatives will result in the desired synergies or efficiencies. Furthermore, management has dedicated, and will continue to dedicate, significant time and effort to implementing such realignment initiatives. These efforts may divert management' s focus and resources from our core business, other corporate initiatives, or strategic opportunities. We may also experience a loss of continuity, loss of accumulated knowledge, or inefficiency during transitional periods. Additionally, efforts related to the implementation of these initiatives could yield unintended consequences (e. g., adversely affecting our ability to execute on merger and acquisition objectives, confusion or distraction of our management and employees, reduced employee morale and retention, delaying the development and introduction of new products and technologies), which may negatively affect our business, sales, financial condition and results of operations.~~ Our international operations expose us to additional risks, and changes in global economic and political conditions could adversely affect our international operations, our revenue and our net income. Approximately 41 % of our total fiscal ~~2023~~ **2024** revenue ~~,~~ was generated from sales outside North America. Political and / or financial instability, oil price shocks and armed conflict in various regions of the world, including, but not limited to, Russia ~~/ ' s invasion of~~ Ukraine **conflict** and the **armed conflicts involving** Israel ~~- Hamas conflict~~ , can lead to economic uncertainty and may adversely impact our business. Political instability may lead to significant, continuing volatility in global stock markets and currency exchange rate fluctuations. If customers' buying patterns, decision- making processes, timing of expected deliveries and timing of new projects unfavorably change due to economic or political conditions, there would be a material adverse effect on our business, financial condition and operating results. Other potential risks inherent in our international business include: • longer payment cycles; • credit risk and higher levels of payment fraud; • greater difficulties in accounts receivable collection; • varying regulatory and legal requirements; • compliance with international and local trade, labor and export control laws; • restrictions on the transfer of funds; • difficulties in developing, staffing, and simultaneously managing a large number of varying foreign operations as a result of distance, legal impediments and language and cultural differences; • reduced or minimal protection of intellectual property rights in some countries; • laws and business practices that favor local competitors or prohibit foreign ownership of certain businesses; • changes in U. S. or foreign trade policies or practices that increase costs or restrict the distribution of products; • seasonal reductions in business activity during the summer months in Europe and certain other parts of the world; • economic instability in emerging markets; and • potentially adverse tax consequences. Any one or more of these factors could have a material adverse effect on our international operations, and, consequently, on our business, financial condition and operating results. In addition, our business has been, and could in the future be, adversely affected by regional or global health crises. A significant outbreak of contagious diseases ~~and~~ **,** other adverse public health developments, or the fear of such events that results in a widespread health crisis could adversely affect global supply chains and the economies and financial markets of many countries. Any prolonged economic disruption could affect demand for our products and services and adversely impact our **business,** ~~results of operations and~~ financial condition **and**

results of operations . If our security measures are breached, our products and services may be perceived as not being secure, customers may curtail or stop using our products and services, and we may incur significant legal and financial exposure ~~.~~ **,** including but not limited to from loss of customer or company data, loss of customers or otherwise. Our products and services involve the storage and transmission of our customers' proprietary information and may be vulnerable to unauthorized access, computer viruses, cyber- attacks, distributed denial of service attacks and other disruptive problems. ~~As~~ **Individual and groups of hackers and sophisticated organizations, including state- sponsored organizations or nation- states, continuously undertake attacks that pose threats to our customers and our software products, and we have experienced cybersecurity incidents in which such actors have gained unauthorized access to our IT systems and data, including customer systems and data. For example, as** disclosed on December 19, 2022, following the detection of irregular activity on certain portions of our corporate network, we engaged outside cybersecurity experts and other incident response professionals to conduct a forensic investigation and assess the extent and scope of the cyber incident (the" November 2022 Cyber Incident"). During the investigation, we and our external advisors uncovered evidence of unauthorized access to our corporate network, including evidence that certain company data had been exfiltrated. As demonstrated by the November 2022 Cyber Incident, due to the actions of outside parties, employee error, malfeasance, or otherwise, an unauthorized party may obtain access to our data or our customers' data, which could result in its theft, destruction, corruption or misappropriation and thus legal and financial exposure. Security risks in recent years have increased significantly given the increased sophistication and activities of hackers, organized crime, including state- sponsored organizations and nation- states, and other outside parties. Cyber threats are continuously evolving, increasing the difficulty of defending against them. Increased risks of such attacks and disruptions also exist due to the Russian invasion of Ukraine beginning in February 2022. While we have implemented security procedures and controls aimed at addressing these threats, our security measures could be compromised, could prove to be inadequate or could fail. Any security breach or unauthorized access could result in significant legal and financial exposure, increased costs to defend litigation, indemnity and other contractual obligations, government fines and penalties, damage to our reputation and our brand, and a loss of confidence in the security of our products and services that could potentially have an adverse effect on our business and results of operations. Breaches of our network could disrupt our internal systems and business applications, including services provided to our customers. Additionally, data breaches could compromise technical and proprietary information, harming our competitive position. We may need to spend significant capital or allocate significant resources to protect against the threat of security breaches or to address security related concerns. If an actual or perceived breach of our security occurs, the market perception of the effectiveness of our security measures could be harmed and we could lose customers. In addition, our insurance coverage may not be adequate to cover all costs related to cybersecurity incidents and the disruptions resulting from such events. If our products contain software defects or security flaws, it could harm our revenues by causing us to lose customers and could increase our liabilities by exposing us to costly governmental investigations or litigation. For example, the exploitation of the zero- day MOVEit Vulnerability in May 2023 has resulted in informal government inquiries, three formal government investigations, and private litigation. Our products, despite extensive testing and quality control, may, and at times do, contain defects, vulnerabilities or security flaws. In the ordinary course of business, we may need to issue corrective releases of our software products to fix any defects, vulnerabilities, or security flaws. Depending upon the severity of any such matters, the detection and correction of such matters can be time consuming and costly. If any such issues are exploited by malicious threat actors, we could experience, among other things, material adverse impact to our revenues due to loss of customers and increased liabilities due to costly governmental investigations or litigation. In addition, any such matters could affect the ability of our products to work with hardware or other software products, delay the development or release of new products or new versions of products (due to a reallocation of our internal resources), and / or adversely affect market acceptance of our products, all of which could have a material adverse effect on our operating results and cash flows. ~~For example, during the third quarter of 2023, we released patches for vulnerabilities affecting WS_FTP, one of our file- transfer products that is deployed on- premise in our customers' environments. Notwithstanding our efforts to promptly patch such vulnerabilities and encourage customers to deploy the patch as quickly as possible, we do not have telemetry into our WS_FTP customers' environments or control over their patching activity, and there have been reports of exploitation of these vulnerabilities following the release of our security patches.~~ As **previously** disclosed ~~via a Form 8- K filed on June 5, 2023~~ , on the evening of May 28, 2023 ~~(Eastern Time)~~ , **we learned that** our ~~MOVEit technical support team received an initial customer support call indicating unusual activity within their MOVEit Transfer instance. An investigative team was mobilized and, on May 30, 2023, the investigative team discovered a zero- day vulnerability in MOVEit Transfer (including our cloud- hosted version of MOVEit Transfer known as MOVEit Cloud). The investigative team determined the zero- day vulnerability (the " MOVEit Vulnerability ") could provide for unauthorized escalated privileges and access to the customer' s underlying environment in both~~ MOVEit Transfer (the on- premise version) and MOVEit Cloud (a cloud- hosted version of MOVEit Transfer **) products were attacked via a" zero- day vulnerability"** that ~~we deploy in both (i) a public cloud~~ **could provide** ~~format, as well as (ii)~~ for **unauthorized escalated privileges** ~~a small group of customers, in customer- dedicated cloud instances that are hosted, separate~~ and **access to** ~~apart from the public instances of our MOVEit Cloud platform). We promptly took down MOVEit Cloud for further investigation and notified all then~~ **the** ~~known current and former MOVEit Transfer and MOVEit Cloud customers in order to apprise them of the MOVEit Vulnerability and alert them to immediate remedial actions. In parallel, our team developed a patch for all supported versions of MOVEit Transfer and MOVEit Cloud, which was released on May 31, 2023, and allowed for the restoration of MOVEit Cloud that same day. MOVEit Transfer is a secure file- transfer software that is installed by customers on- premise and does not have any on- going telemetry after installation that allows us to track, among other things, a~~ customer' s **underlying environment** ~~product usage, deployed version, file transfer activity (including any data~~ **the" MOVEit Vulnerability"). A" zero- day vulnerability" is a vulnerability** that ~~is transferred~~ **has been publicly disclosed and / or exploited (e. g.,** by **an independent researcher or threat actor) before the software vendor has**

an opportunity to patch it. We continue to monitor the impact of the MOVEit Vulnerability on ~~or~~ **our** ~~stored within the customer's~~ **business, operations, and financial results.** MOVEit Transfer **and** ~~instance), or whether the customer has applied any security patches or bug fixes to their~~ MOVEit ~~Transfer instance. However~~ **Cloud represented less than 4 % in aggregate of our revenue for the fiscal year ended November 30** , **2024. As** a ~~number~~ **result** of ~~MOVEit Transfer customers and others have disclosed that malicious threat actors have exploited~~ the MOVEit Vulnerability ~~to obtain access to their environments and portions of their sensitive customer data. We have not seen any evidence that sensitive customer data has been exfiltrated from the public MOVEit Cloud instances. For a small group of customers~~ , ~~we provide dedicated MOVEit Cloud instances that are hosted, for each such customer, separate and apart from the public instances of our MOVEit Cloud platform. Two of our dedicated MOVEit Cloud customers have reported that malicious threat actors have exploited the MOVEit Vulnerability to obtain access to their dedicated MOVEit Cloud environment. As of the date of the filing of this report on Form 10- K, one such customer has confirmed that no sensitive data was compromised and the other has reported that certain personally identifiable information was exfiltrated. As of the date of the filing of this report on Form 10- K, (i) we have received formal letters from 31 customers and others that claim to have been impacted by the MOVEit Vulnerability, some of which have indicated that they intend to seek indemnification from us related to the MOVEit Vulnerability, (ii) we have received a letter from an insurer providing notice of a subrogation claim (where the insurer is seeking recovery for all expenses incurred in connection with the MOVEit Vulnerability), which has resulted in the filing of a lawsuit in the United States District Court for the District of Massachusetts (" District of Massachusetts"), and (iii)~~ we are party to **certain** ~~approximately 118~~ class action lawsuits filed by individuals who claim to have been impacted by **the** exfiltration of data from the environments of our MOVEit Transfer customers, which the Judicial Panel on Multidistrict Litigation transferred to the District of Massachusetts for coordinated and consolidated proceedings **(the" MDL"). The MDL has also consolidated the previously disclosed insurance subrogation claim (where an insurer is seeking recovery for expenses incurred on behalf of its insured in connection with the MOVEit Vulnerability) and, as of the date of this filing, one customer cross- claim** . We have also been cooperating with ~~several inquiries~~ - **inquires** ~~from domestic~~ and ~~foreign data privacy regulators; inquiries from several state attorneys general; as well as formal~~ investigations from: (i) **several domestic and foreign data privacy regulators (as of the date of this filing, we have assisted with all inquiries and investigations, a number of which have been formally closed without regulatory action), (ii) several state attorneys general (as of the date of this filing, we have assisted with all inquiries and investigations, and are not aware of any enforcement or regulatory actions directed against Progress), (iii)** a U. S. federal law enforcement agency (as of the date of ~~the~~ **this** filing ~~of~~ **, we have assisted with all inquiries under** this ~~report, the law enforcement~~ investigation **and this** ~~that we are cooperating with~~ is not an enforcement action or formal governmental investigation ~~of which we have been told that we are a target~~ **targeting Progress**), **and** (~~ii~~ **iv**) ~~the SEC (as further described hereafter), and (iii) the Office of the Attorney General for the District of Columbia (as further described hereafter); all of which could have adverse impacts~~ on ~~our business and operations and the results thereof. On October 2, 2023, we received a subpoena from the SEC seeking various documents and information relating to the MOVEit Vulnerability. As described in the cover letter accompanying the subpoena, at this stage, the SEC investigation is a fact- finding inquiry, the investigation does not mean that Progress or anyone else has violated federal securities laws, and the investigation does not mean that the SEC has a negative opinion of any person, entity, or security. Progress intends to cooperate fully with the SEC in its investigation. On~~ December 21, 2023, we received a preservation notice from the Federal Trade Commission (the" FTC"), but have not otherwise received a request for information **,** nor is Progress aware of any formal FTC investigation. ~~On January 18~~ **In addition to the above** , ~~2024~~ **and as disclosed in prior filings** , we received a subpoena from the ~~Office~~ **SEC' s Division** of **Enforcement on October 2** ~~the Attorney General for the District of Columbia seeking various documents and information relating to the MOVEit Vulnerability. At this stage~~ , ~~the investigation is~~ **2023, as part of** a fact- finding inquiry ~~,~~ **seeking various documents** and **information relating to** the ~~investigation does not mean~~ **MOVEit Vulnerability. In a letter dated August 7, 2024, the SEC notified us** that **it had concluded** ~~Progress or anyone else has violated applicable laws. Progress intends to cooperate fully with the Office of the Attorney General for the District of Columbia in~~ its investigation **and did not intend to recommend an enforcement action against us (the" Termination Letter")** . **The Termination Letter was provided under the guidelines set out in the final paragraph of Securities Act Release No. 5310. Our financial liability arising from any of the foregoing will depend on many factors, including the progression of the MDL; therefore, we are unable at this time to estimate the quantitative impact of any** ~~Such~~ **such liability with any reasonable degree of certainty. As our litigation response continues, we will continue to assess the potential impact of the MOVEit Vulnerability on our business, operations, and financial results. The** claims and investigations **described above** may have an adverse effect on how we operate our business and our results of operations, and in the future, we may be subject to additional governmental or regulatory investigations, as well as additional litigation or indemnification claims **related to the MOVEit Vulnerability** . Following the discovery of the MOVEit Vulnerability and the various remedial actions **previously** described ~~here~~ , we have discovered and patched additional vulnerabilities within the MOVEit Transfer and MOVEit Cloud platforms. While we are currently not aware of any evidence that these additional vulnerabilities were exploited by malicious threat actors, we cannot guarantee that we have or will uncover and / or address all vulnerabilities within the MOVEit platform or any of our other products prior to exploitation by threat actors. Our ~~financial liability arising from any of the foregoing will depend on many factors, including the extent to which governmental entities investigate the matter and limitations contained within our customer contracts; therefore, we are unable at this time to estimate the quantitative impact of any such liability with any reasonable degree of certainty. As our fact- gathering investigation and litigation response continues, we will continue to assess the potential impact of the MOVEit Vulnerability on our business, operations, and financial results. Also, each of the governmental inquiries and investigations mentioned above could result in adverse judgements, settlements, fines, penalties, or other resolutions, the amount, scope and timing of which could be material, but which we are currently unable to predict. Our~~ business could be damaged, and we could be subject to

liability, in the event of any unauthorized access to our data or our customers' data, including through privacy and data security ~~breaches~~ -- **breach** ~~, such as or in addition to the MOVEit Vulnerability~~ . The use of certain of our products, including MOVEit Cloud **and ShareFile** , involves the transmission or storage of third- party data in our environment, some of which may be considered personally identifiable, confidential, or sensitive. In the ordinary course of business, we face security threats from malicious threat actors that could obtain unauthorized access to our systems, infrastructure, products, and networks. We anticipate that these threats will continue to grow in scope and complexity over time ~~. For example , once~~ **particularly as** we **acquire new products** ~~discovered the MOVEit Vulnerability on May 30, 2023, we (i) promptly took down MOVEit Cloud for investigation,~~ and ~~(ii) notified all then- known current and former MOVEit Transfer and MOVEit Cloud customers in order to apprise them of the MOVEit Vulnerability and alert them to immediate remedial actions. In parallel, our team developed~~ a **larger proportion** ~~patch for all supported versions~~ of **our revenues derive from products** ~~MOVEit Transfer and MOVEit Cloud, which was released on May 31, 2023 and allowed for the restoration of MOVEit Cloud~~ that ~~same day~~ **transmit or store sensitive data** . While we **endeavor to** ~~believe that our actions have, and will~~ continue **mitigating security risks for** ~~to, reduce the likelihood of similar vulnerabilities occurring in the future in~~ our ~~MOVEit product~~ **products** ~~line~~ , malicious threat actors might use techniques to exploit other zero- day vulnerabilities or use other means that we are unable to defend against, in order to compromise and infiltrate our systems, infrastructure, networks, and products, including, but not limited to, MOVEit **, ShareFile** or other products ~~. In addition, MOVEit Transfer is a secure file- transfer software that is installed by customers on- premise and does not have any on- going telemetry after installation that allows us to track, among other things, a customer' s product usage, deployed version, file transfer activity (including any data that is transferred by or stored within the customer' s MOVEit Transfer instance), or whether the customer has applied any security patches or bug fixes to their MOVEit Transfer instance~~ . While we devote ~~a~~ significant ~~amount of~~ resources to cyber security related matters in the operation of our business, we may fail to detect the existence of a breach and be unable to prevent unauthorized access to user and company content across our systems, infrastructure, products, and networks. The techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently and are often not recognized until launched against a target. They may originate from less regulated or remote areas around the world, or from state- sponsored actors. If our security measures are breached, we may suffer reputational damage, our products may be perceived as insecure, and we may lose existing customers ~~,~~ or fail to attract and retain new customers. In addition to internal resources, we frequently rely on third parties when deploying our cybersecurity related infrastructure, and in doing so, may be exposed to security risks outside of our direct control. In connection therewith, we rely on outside vendors and contractors to perform certain services necessary for the operation and testing of certain of our products, and they may fail to adequately secure our platform or discover vulnerabilities in our products. While we have implemented security procedures and controls aimed at addressing these threats and patching vulnerabilities, our security measures could be compromised and our attempts to implement security measures and patch vulnerabilities could prove to be inadequate or could fail. Any such failure could result in significant legal and financial exposure, increased costs to defend litigation, indemnity and other contractual obligations, government fines and penalties, damage to our reputation and our brand, and a loss of confidence in the security of our products and services that could potentially have an adverse effect on our business and results of operations. In addition, our insurance coverage may not be adequate to cover all costs related to cybersecurity incidents or the exploitation of vulnerabilities as well as the disruptions and liabilities resulting from such events. A failure of our information technology systems, including a cyber incident, could have a material adverse effect on our business. We rely on our technology infrastructure, and the technology infrastructure of third parties, for many functions, including selling our products, supporting our ISVs and other third- party channels, fulfilling orders and billing, and collecting and making payments. This technology infrastructure may be vulnerable to damage or interruption from natural disasters, power loss, telecommunication failures, terrorist attacks, the outbreak of wars or other armed conflicts, the escalation of hostilities, geopolitical tensions or trade wars, acts of terrorism or ~~" "~~ acts of God, ~~" "~~ particularly involving geographies in which we or third parties on whom we depend have operations, computer intrusions or other similar cyber intrusions, vulnerabilities and viruses, software errors, computer denial- of- service attacks and other similar events. A significant number of the systems making up this infrastructure are not redundant, and our disaster recovery planning may not be sufficient for every eventuality. This technology infrastructure may fail or be vulnerable to damage or interruption because of actions by third parties or employee error or malfeasance. In addition, depending upon the severity of any such actions, we may not carry business interruption insurance sufficient to protect us from all losses that may result from interruptions in our services as a result of such technology infrastructure failures or provide us with the ability to cover all contingencies. Any interruption in the availability of our websites and on- line interactions with customers or partners may cause a reduction in customer or partner satisfaction levels, which in turn could cause additional claims, reduced revenue or loss of customers or partners. Despite any precautions we may take, these problems could result in, among other consequences, a loss, destruction, corruption or misappropriation of company or customer data, loss of confidence in the stability and reliability of our offerings, damage to our reputation, and legal liability, all of which may adversely affect our business, financial condition, operating results and cash flows. **.** Integration of artificial intelligence into our product offerings and our use of artificial intelligence in our operations could result in reputational or competitive harm,legal liability,and other adverse effects on our business.We have integrated,and plan to further integrate, ~~artificial intelligence (" AI ")~~ capabilities into certain components of product offerings,and we ~~use and~~ expect to ~~increase the~~ use ~~of~~ AI in our operations.Such integration and use of AI may become more important in our product offerings and operations over time.These AI- related initiatives,whether successful or not,could cause us to incur substantial costs and could result in delays in our software release cadence.Our competitors or other third parties may incorporate AI into their products or operations more quickly or more successfully than we do,which could impair our ability to compete effectively.Additionally,AI algorithms may be flawed and datasets underlying AI algorithms may be insufficient or contain biased information.If the AI tools integrated into our products or that we use in our operations produce analyses or recommendations that are or are alleged to be

deficient,inaccurate,or biased,our reputation,business,financial condition,and results of operations may be adversely affected.Other companies have experienced cybersecurity incidents that implicate confidential and proprietary company data and / or the personal data of end users of AI applications integrated into their software offerings or used in their operations.If we were to experience a cybersecurity incident **,whether** related to the integration of AI capabilities into our product offerings or our use of AI applications in our operations,our business and results of operations could be adversely affected.AI also presents various emerging legal,regulatory and ethical issues,and the incorporation of AI into our product offerings and our use of AI applications in our operations could require us to expend significant resources in developing,testing and maintaining our product offerings and may cause us to experience brand,reputational,or competitive harm,or incur legal liability.On October 30,2023,the Biden administration issued an Executive Order to,among other things,establish extensive new standards for AI safety and security.Other jurisdictions may decide to adopt similar or more restrictive legislation that may render the use of such technologies challenging.These restrictions may make it harder for us to conduct our business using AI,lead to regulatory fines or penalties,require us to change our product offerings or business practices, **or prevent or limit our use of AI** Catastrophic events, including but not limited to cyber events, may disrupt our business. We rely on our network infrastructure and enterprise applications, internal technology systems and website for our development, marketing, operations, support and sales activities. In addition, we rely on third- party hosted services, and we do not control the operation of third- party data center facilities, which increases our vulnerability. A disruption, infiltration or failure of these systems or third- party hosted services in the event of a major earthquake, fire, flood, tsunami or other weather event, power loss, telecommunications failure, software or hardware ~~malfunctions~~ **malfunction** , ~~pandemics~~ **pandemic** , cyber- attack or other similar ~~interruptions~~ **interruption** to our business, war, terrorist attack or other catastrophic event that our disaster recovery plans do not adequately address, could cause system interruptions, reputational harm, loss of intellectual property, delays in our product development, lengthy interruptions in our services, breaches of data security and loss, destruction, misappropriation or corruption of critical company or customer data. A catastrophic event ~~including a cyber event a war or an act of terrorism~~ that results in the loss, destruction, misappropriation, corruption or disruption of any of our data, our ~~customer~~ **customers** ' ~~s~~ data or our data centers or our critical business or information technology systems could severely affect our ability to conduct normal business operations and, as a result, our future operating results could be adversely affected, and the adverse effects of any such catastrophic event would be exacerbated if experienced at the same time as another unexpected and adverse event. **We also depend on third- party service providers to provide the data centers and other infrastructure necessary to certain of our products. Any disruption in the services provided by these third parties or any failure to renew the services could adversely affect the performance of products or result in a loss of user content, resulting in harm to our business and reputation. Customers rely on certain of our products to transfer or process their content. The infrastructure on which our products rely may not be adequately designed with sufficient reliability and redundancy to avoid performance delays or outages and / or may not be scalable to meet increasing user demands. If our products are unavailable when users attempt to access them, or if the products do not load or perform as quickly as users expect, they may decrease or discontinue their use of our products, which could be harmful to our business, results of operations, and financial condition. Our third- party service providers along with their datacenters and other facilities are also vulnerable to damage or interruption from human error, intentional bad acts, security breaches and other catastrophic events, any of which could disrupt the availability of our products and / or compromise or destroy user content, which could be harmful to our business, results of operations, and financial condition.** Adverse developments in our relationships with ~~certain third~~ **sales channel** ~~parties~~ **partners** ~~or within the business of such third parties~~ could harm our revenues and results of operations. We recognize a substantial portion of our revenue from sales made through third parties, including our ISVs, distributors / resellers, and OEMs, and our future results depend in large part upon our continued successful distribution of our products through these channels. The activities of these third parties are not within our direct control. Our failure to manage our relationships with these third parties effectively could impair the success of our sales, marketing and support activities. A reduction in the sales efforts, technical capabilities or financial viability of these parties, a misalignment of interest between us and them, or a termination of our relationship with a major ISV, distributor / reseller, or OEM could have ~~a negative~~ **an adverse** effect on our sales and financial results. Any adverse effect on any of our ISV' s, distributors' / resellers', or OEMs' businesses related to competition, pricing and other factors could also have a material adverse effect on our business, financial condition and operating results. Our customers and partners may seek refunds, delay implementation timelines, delay payment, fail to pay us in accordance with the terms of their agreements, **decline renewals or upgrades, or reduce** or terminate use of our products, all of which can have an adverse effect on us. ~~If~~ **Customers and partners may not renew or reduce their use of our products due to various factors, such as dissatisfaction with our products (including features, user experience, or support), pricing, no longer having a need for our products, the availability of competitive products, or the impact of macroeconomic trends or catastrophic events. Our business depends on our ability to retain and expand relationships with customers, and any decline in renewals or failure to expand business relationships with customers consistent with our past experience could adversely affect our future results of operations. Moreover, if** customers or partners seek refunds, delay implementation of our products, delay payment, fail to pay us under the terms of our agreements, or terminate use of our products, we may be adversely affected both from the inability to collect amounts due and the cost of enforcing the terms of our contracts (including litigation related thereto). ~~For example, as of the date of the filing of this report on Form 10- K, 31 customers and others that claim to have been impacted by the MOVEit Vulnerability have indicated that they intend to seek indemnification from us related to the MOVEit Vulnerability and it is possible that, in connection therewith, they may delay payment under the terms of their contracts. Other MOVEit Transfer and MOVEit Cloud customers have sought refunds or delayed implementation timelines. As the scope of the impact of the MOVEit Vulnerability becomes more clear, additional customers may attempt to seek refunds, delay product implementation, withhold payments, or cease using the MOVEit product line entirely.~~ In addition, in the ordinary course of

business, some of our customers and partners may seek bankruptcy protection or other similar relief and fail to pay amounts due to us, or pay those amounts more slowly, either of which could adversely affect our operating results, financial position and cash flow. We rely on the experience and expertise of our skilled employees, and must continue to attract and retain qualified technical, marketing and managerial personnel in order to succeed. Our future success will depend in large part upon our ability to attract and retain highly skilled technical, managerial, sales and marketing personnel. There is significant competition for such personnel in the software industry. We may not continue to be successful in attracting and retaining the personnel we require to develop new and enhanced products and to continue to grow and operate profitably. **We have relationships with third parties to provide, develop, and create applications that integrate with certain of our products, and our business could be harmed if we are unable to continue these relationships. We use software and services licensed and procured from third parties. We may need to obtain additional licenses and services from third parties to utilize the intellectual property and technology associated with the development of our products, which might not be available to us on acceptable terms, or at all. Any loss of the right to use any software or services required for the development and maintenance of our products could harm our business. Any errors or defects in third- party software or services could result in errors or a failure of our products, which could harm our business, results of operations, and financial condition. Certain of our products depend on interoperability with various devices, operating systems, and third- party applications that we do not control. An important feature of many of our products is their compatibility with a wide range of devices, operating systems, and third- party applications. Such products depend on accessibility across these third- party systems and applications, which are constantly evolving and usually outside of our control. We may not always be able to modify our products to ensure compatibility with these third- party services following their updates and upgrades. If we cannot ensure compatibility, our business, results of operations, and financial condition could be adversely affected.** Risks Related to Laws and Regulations We are subject to risks associated with compliance with laws and regulations globally, which may harm our business. We are a global company subject to varied and complex laws, regulations and customs, both domestically and internationally. These laws and regulations relate to **many core** ~~a number of~~ aspects of our business, including ~~trade protection, import and export control, data and transaction processing security, payment card industry data security standards, records management, user- generated content hosted on websites we operate,~~ data privacy or related privacy practices, **AI** ~~data residency~~ , corporate governance **, securities regulations** , anti- trust and competition, ~~employee and third- party complaints,~~ anti- corruption, **sanctions** ~~gift policies, conflicts of interest, securities regulations~~ and ~~other regulatory requirements affecting~~ trade **protection,** and ~~investment~~ **import and export control** . The application of these laws and regulations to our business is often unclear and may at times conflict on a domestic or international basis. For example, **data privacy and AI regulations are evolving rapidly** in many **jurisdictions** ~~foreign countries~~ , **often** ~~particularly in those~~ with **extremely punitive penalties** ~~developing economies, it is common to engage in business practices that are prohibited by U. S. regulations applicable to us, including the Foreign Corrupt Practices Act. We cannot provide assurance that our employees, contractors, agents and business partners will not take actions in violation of our internal policies or U. S. laws~~ . Compliance with these laws and regulations may involve significant costs or require changes in our business practices that result in reduced revenue and profitability. Non- compliance could also result in fines, damages, criminal sanctions against us, our officers or our employees, prohibitions on the conduct of our business, and damage to our reputation ~~. In response to the Russian invasion of Ukraine, sanctions have been imposed by the U. S., Canada, the United Kingdom, the European Union, and other countries and companies and organizations against officials, individuals, regions, and industries in Russia and Ukraine. Although we have policies and procedures in place that are designed to comply with applicable sanctions, our employees, contractors, and agents may take actions in violation of such policies and applicable law and ultimately we could be held responsible. If we are held responsible for a violation of U. S. sanctions laws, we may be subject to various penalties, any of which could have a material adverse effect on our business, financial condition or results of operations~~ . Our business practices with respect to the collection, use and management of personal information could give rise to operational interruption, liabilities or reputational harm as a result of governmental regulation, legal requirements or industry standards relating to consumer privacy and data protection. As regulatory focus on privacy issues continues to increase and worldwide laws and regulations concerning the handling of personal information expand and become more complex, potential risks related to data collection and use within our business will intensify. For example, the regulatory environment applicable to the handling of the European Economic Area (" EEA") residents' personal data, which is governed by the General Data Protection Regulation of 2018 (~~“~~ **"** GDPR ~~”~~ **"**) and / or respectively the national data protection laws of United Kingdom, Switzerland, and other countries **in which** we operate, may cause us to assume additional liabilities, obligations or incur additional costs, and could result in our business, operating results and financial condition being harmed. Additionally, we and our customers may face a risk of enforcement actions by the competent data protection authorities relating to personal data transfers to us and by us from the EEA and other jurisdictions which have country specific data transfer requirements. Any such enforcement actions could result in substantial costs and diversion of resources, distract management and technical personnel and ~~negatively~~ **adversely** affect our business, operating results and financial condition. In addition, governmental entities in the U. S. and other countries have enacted or are considering enacting legislation or regulations or may in the near future interpret existing legislation or regulations, in a manner that could significantly impact our ability and the ability of our customers and data partners to collect, augment, analyze, use, transfer and share personal and other information that is integral to certain business functions. For example, ~~the California Consumer~~ **U. S. states like Texas and Oregon enacted data** ~~Privacy~~ **privacy laws that** ~~Act (as amended by the California Privacy Rights Act)~~ took effect **in** ~~on January 1, 2023~~ **2024** ~~and~~ **, both of which** expanded the consumer ~~'~~ **'** s privacy rights and the obligations to the organizations doing business in ~~California~~ **those states** . Other U. S. state legislatures have also implemented varying privacy laws and regulations, or are considering implementing legislation that we expect to become effective in the near term. Moreover, several privacy bills are under congressional review at the U. S. federal level. Changes in laws or regulations associated with the

enhanced protection of certain types of sensitive data, such as healthcare data or other personal information, could greatly increase our cost of providing our products and services or even prevent us from offering certain services in jurisdictions that we operate. Regulators globally are also imposing greater monetary fines for privacy violations (e. g., non- compliance with the GDPR may result in monetary penalties of up to 4 % of worldwide revenue). Additionally, public perception and standards related to the privacy of personal information can shift rapidly, in ways that may affect our reputation or influence regulators to enact regulations and laws that may limit our ability to provide certain products. Any failure, or perceived failure, by us to comply with U. S. federal, state, or international laws and regulations, including laws and regulations regulating privacy, data security, or consumer protection, or other policies, public perception, standards, self- regulatory requirements or legal obligations, could result in lost or restricted business, proceedings, actions or fines brought against us or levied by governmental entities or others, or could adversely affect our business and harm our reputation. We could incur substantial cost in protecting our proprietary software technology and if we fail to protect our technology, we could incur material harm to our business. We rely principally on a combination of contract provisions and copyright, trademark, patent and trade secret laws to protect our proprietary technology. Despite our efforts to protect our proprietary rights, unauthorized parties may attempt to copy aspects of our products or to obtain and use information that we regard as proprietary. Policing unauthorized use of our products is difficult. Litigation may be necessary in the future to enforce our intellectual property rights, to protect our trade secrets or to determine the validity and scope of the proprietary rights of others. This litigation could result in substantial costs and diversion of resources, whether or not we ultimately prevail on the merits. The steps we take to protect our proprietary rights may be inadequate to prevent misappropriation of our technology; moreover, others could independently develop similar technology. We could be subject to claims that we infringe intellectual property rights of others, which could harm our business, financial condition, **and** results of operations ~~or cash flows~~. Third parties could assert infringement claims in the future with respect to our products and technology, and such claims might be successful. Litigation relating to any such claims could result in substantial costs and diversion of resources, whether or not we ultimately prevail on the merits. Any such litigation could also result in our being prohibited from selling one or more of our products, unanticipated royalty payments, reluctance by potential customers to purchase our products, or liability to our customers and could have a material adverse effect on our business, financial condition, **and** operating results and cash flows. Changes in..... a material adverse impact on our financial results. Contracting with government entities exposes us to additional risks inherent in the government procurement process. We provide products and services, directly and indirectly, to a variety of government entities, both domestically and internationally. Risks associated with licensing and selling products and services to government entities include more extended sales and collection cycles, varying governmental budgeting processes and adherence to complex procurement regulations and other government- specific and contractual requirements, including with respect to ongoing compliance. We may be subject to audits and investigations relating to our government contracts and any violations could result in various civil and criminal penalties and administrative sanctions, including termination of contracts for default or for the convenience of the government, payment of fines, and suspension or debarment from future government business, as well as harm to our reputation and financial results. Risks Related to Financial Performance or General Economic Conditions Weakness in the U. S. and international economies may result in fewer sales of our products and may otherwise harm our business. We are subject to risks arising from adverse changes in global economic conditions, especially those in the U. S., Europe and Latin America. If global economic conditions weaken, credit markets tighten and / or financial markets become unstable, customers may delay, reduce or forego technology purchases, both directly and through our ISVs, resellers / distributors and OEMs. This could result in reductions in sales of our products, longer sales cycles, slower adoption of new technologies and increased price competition. Further, deteriorating economic conditions could adversely affect our customers and their ability to pay amounts owed to us (see Our customers and partners may seek refunds, delay implementation timelines, delay payment, fail to pay us in accordance with the terms of their agreements, **decline renewals or upgrades, or reduce** or terminate use of our products, all of which can have an adverse effect on us). ~~The~~ **If the** U. S. and other international economies ~~continue to~~ experience inflationary pressures, ~~which may increase~~ our expenses (including the cost of labor) **may increase**, ~~negatively affect~~ credit and securities markets ~~generally~~ **may be adversely affected**, and ~~further impact~~ customer demand for our products and their ability to make payments **may be impacted**. Any of these events would likely harm our business, ~~results of operations,~~ financial condition ~~or cash flows~~ **, and results of operations**. We are currently operating in a period of economic uncertainty and capital markets disruption due to various geopolitical and macro- economic factors, which may materially adversely affect our business, financial condition, and results of operations ~~. U. S. and global markets are continuing to experience volatility and disruption following among other things the escalation of geopolitical tensions in February 2022 with Russia' s invasion of Ukraine and the recent Israel- Hamas conflict~~. The overall macro global economy, including ~~the~~ ongoing military ~~conflict~~ **conflicts** in Ukraine and the Middle East, ~~is highly~~ **and increasing tensions between the U. S. and China, remain** unpredictable and has already led to market disruptions, including volatile capital markets, higher interest rates and debt capital costs, diminished liquidity and credit availability, declines in consumer confidence and discretionary spending, as well as supply chain disruptions and increases in costs of certain raw materials and transportation, which have in turn contributed to global inflationary pressures. ~~These and related actions, responses, and consequences may contribute to world- wide economic downturns. In addition, prolonged~~ **Prolonged** unrest, military activities, or broad- based sanctions could have a material adverse effect on our operations and business outlook. Given our meaningful reliance on revenue generated outside of North America (which constituted 41 % of our total revenue in fiscal ~~2023~~ **2024**) and our reliance on revenue generated in EMEA (which constituted ~~32~~ **33** % of our total revenue in fiscal ~~2023~~ **2024**), disruption of commercial activities in these regions may materially adversely affect our financial condition and results of operations. Although we cannot predict what the impacts may be, our global operations and reliance on interconnected technology increase the risk to our operations ~~. The extent and duration of the conflict in Ukraine and the Middle East, geopolitical tensions, inflationary pressures and resulting market disruptions are impossible to predict but could be substantial~~.

Fluctuations in foreign currency exchange rates or interest rates have had, and could continue to have, an adverse impact on our financial condition and results of operations. Changes in the value of foreign currencies relative to the U. S. dollar and related changes in interest rates have adversely affected our results of operations and financial position and could continue to do so. In recent periods, as the value of the U. S. dollar has strengthened in comparison to certain foreign currencies (particularly in EMEA), our reported international revenue has been reduced because foreign currencies translate into fewer U. S. dollars. As approximately one- third of our revenue is denominated in foreign currencies, these exchange rate fluctuations have impacted, and we expect will continue to impact, our revenue results. Please see Management' s Discussion and Analysis of Financial Condition and Results of Operations in Part II, Item 7 for additional information. We seek to reduce our exposure to fluctuations in exchange rates by entering into foreign exchange forward contracts to hedge certain actual and forecasted transactions of selected currencies (mainly in Europe, Brazil, India and Australia); however, our currency hedging transactions may not be effective in reducing the adverse impact of fluctuations in foreign currency exchange rates. Further, as geopolitical volatility around the world increases, there is increasing risk of the imposition of exchange or price controls, or other restrictions on the conversion of foreign currencies, which could have a material adverse effect on our business **, financial condition and operating results** . Revenue forecasting is uncertain, and the failure to meet our forecasts could result in a decline in **the market price of** our **common** stock ~~price~~ . Our revenues, particularly new software license revenues or economic impacts from M & A activities, are difficult to forecast. We use a pipeline system to forecast revenues and trends in our business. Our pipeline estimates may prove to be unreliable either in a particular quarter or over a longer period of time, in part because the conversion rate of the pipeline into contracts can be difficult to estimate and requires management judgment. A variation in the conversion rate could cause us to plan or budget incorrectly and result in a material adverse impact on our business or our planned results of operations. Furthermore, most of our expenses are relatively fixed, including costs of personnel and facilities. Thus, an unexpected reduction in our revenue, or failure to achieve the anticipated rate of growth or realize synergies from M & A activity, would have a material adverse effect on our profitability. If our operating results do not meet our publicly stated guidance or the expectations of investors or analysts, **the market price of** our **common** stock ~~price~~ may decline. Our revenue and quarterly results may fluctuate, which could adversely affect **the market price of** our **common** stock ~~price~~ . We have experienced, and may in the future experience, significant fluctuations in our quarterly operating results that may be caused by many factors. These factors include: • changes in demand for our products; • introduction, enhancement or announcement of products by us or our competitors; • market acceptance of our new products, including acquired products; • the growth rates of certain market segments in which we compete; • size and timing of significant orders; • a high percentage of our revenue is generated in the third month of each fiscal quarter and any failure to receive, complete or process orders at the end of any quarter could cause us to fall short of our revenue targets; • budgeting cycles of customers; • mix of distribution channels; • mix of products and services sold; • mix of international and North American revenues; • fluctuations in currency exchange rates; • changes in the level of operating expenses, including unforeseen expenses incurred in connection with items such as cyber security instances; • changes in management; • restructuring programs; • changes in our sales force; • completion or announcement of acquisitions by us or our competitors; • integration of acquired businesses or inability to realize expected synergies; • customer order deferrals in anticipation of new products announced by us or our competitors; • general economic conditions in regions in which we conduct business; and • other factors such as political or social unrest, terrorist attacks, other hostilities, natural disasters, cyber- attacks, and potential public health crises, such as pandemics. ~~Our common stock price may continue to be volatile, which could result in losses for investors.~~ The market price of our common stock, like that of other technology companies, is volatile and is subject to wide fluctuations in response to quarterly variations in operating results, announcements of technological innovations or new products by us or our competitors, changes in financial estimates by securities analysts or other events or factors. ~~Our~~ **The market price of our common** stock ~~price~~ may also be affected by broader market trends unrelated to our performance. As a result, purchasers of our common stock may be unable at any given time to sell their shares at or above the price they paid for them. **results and cash flows.** Changes in accounting principles and guidance,or their interpretation or implementation,may materially adversely affect our reported results of operations or financial position.We prepare our consolidated financial statements in accordance with accounting principles generally accepted in the United States of America (~~"~~ **“** GAAP ~~"~~ **”**) These principles are subject to interpretation by the SEC and various bodies formed to create and interpret appropriate accounting principles and guidance.A change in these principles or guidance,or in their interpretations,may have a significant effect on our reported results,as well as our processes and related controls.We may have exposure to additional tax liabilities.As a multinational corporation,we are subject to income taxes in the U.S.and various foreign jurisdictions.Significant judgment is required in determining our global provision for income taxes and other tax liabilities.In the ordinary course of a global business,there are many intercompany transactions and calculations where the ultimate tax determination is uncertain.Our income tax returns are routinely subject to audits by tax authorities.Although we regularly assess the likelihood of adverse outcomes resulting from these examinations to determine our tax estimates,a final determination of tax audits that is inconsistent with such assessments or tax disputes could have an adverse effect on our financial condition,results of operations and cash flows.We are also subject to non- income taxes,such as payroll,sales,use,value-added,net worth,property and goods and services taxes in the U.S.and various foreign jurisdictions.We are regularly under audit by tax authorities with respect to these non- income taxes and may have exposure to additional non- income tax liabilities,which could have an adverse effect on our results of operations,financial condition and cash flows.In addition,our future effective tax rates could be favorably or unfavorably affected by changes in tax rates,changes in the valuation of our deferred tax assets or liabilities,or changes in tax laws ~~including Pillar Two legislation adopted as part of the Organization for~~ - **or** ~~Economic Cooperation and Development (“ OECD ”)~~ **their interpretation.Such changes could have a material adverse impact on our financial** Risks Related to our Indebtedness and Convertible Senior Notes Our indebtedness and liabilities could limit the cash flow available for our operations ~~,~~ **and** expose us to risks that could adversely affect our business, financial condition and results

of operations. As of November 30, ~~2023~~ **2024**, we had approximately $ ~~724~~ **1. 5** ~~million~~ **billion** of consolidated indebtedness. We may also incur additional indebtedness to meet future financing needs. Our indebtedness could have significant ~~negative~~ **adverse** consequences for our security holders and our business, results of operations and financial condition by, among other things: • increasing our vulnerability to adverse economic and industry conditions; • limiting our ability to obtain additional financing; • requiring the dedication of a substantial portion of our cash flow from operations to service our indebtedness, which will reduce the amount of cash available for other purposes; • limiting our flexibility to plan for, or react to, changes in our business; • diluting the interests of our existing stockholders as a result of issuing shares of our common stock upon conversion of our Convertible Senior Notes with an aggregate principal amount of $ 360 million, due April 15, 2026 **, and an aggregate principal amount of $ 450 million, due March 1, 2030** (**together,** the" Notes"); and • placing us at a possible competitive disadvantage with competitors that are less leveraged than us or have better access to capital. Our ability to make scheduled payments of the principal of, to pay interest on or to refinance our current or future indebtedness, including the Notes, depends on our future performance, which is subject to economic, financial, competitive and other factors beyond our control. Our business may not generate sufficient funds, and we may otherwise be unable to maintain sufficient cash reserves, to pay amounts due under our current or future indebtedness, including the Notes, and our cash needs may increase in the future. In addition, our credit facility contains, and any future indebtedness that we may incur may contain, financial and other restrictive covenants that limit our ability to operate our business, raise capital or make payments under our other indebtedness. If we fail to comply with these covenants or to make payments under our indebtedness when due, then we would be in default under that indebtedness, which could, in turn, result in that and our other indebtedness becoming immediately payable in full. We are required to comply with certain financial and operating covenants under our Credit Facility and to make scheduled debt payments as they become due; any failure to comply with those covenants or to make scheduled payments could cause amounts borrowed under the facility to become immediately due and payable or prevent us from borrowing under the facility. In ~~January~~ **March** ~~2022~~ **2024**, we entered into a ~~Third~~ **Fourth** Amended and Restated Credit Agreement (the" Credit Agreement"), which provides for a $ ~~275~~ **900**. 0 million **secured** ~~term loan and a $ 300. 0 million~~ revolving credit facility (which may be increased ~~by an additional $ 260. 0 million~~ if the existing or additional lenders are willing to make such increased commitments) (the" Credit Facility"). This Credit Facility matures in ~~January~~ **March** ~~2027~~ **2029**, at which time any amounts outstanding will be due and payable in full. We may wish to borrow additional amounts under the facility in the future to support our operations, including for strategic acquisitions and share repurchases. We are required to comply with specified financial and operating covenants and to make scheduled repayments of our term loan, which may limit our ability to operate our business as we otherwise might operate it. Our failure to comply with any of these covenants or to meet any payment obligations under the facility could result in an event of default which, if not cured or waived, would result in any amounts outstanding, including any accrued interest and unpaid fees, becoming immediately due and payable. We might not have sufficient working capital or liquidity to satisfy any repayment obligations in the event of an acceleration of those obligations. In addition, if we are not in compliance with the financial and operating covenants at the time we wish to borrow funds, we will be unable to borrow funds. ~~We may be required to repay the Credit Agreement prior to the stated maturity date, if the springing maturity feature is triggered. The Credit Agreement has a stated maturity date of January 25, 2027, but includes a springing maturity feature that will cause the stated maturity date to spring ahead to the date that is 181 days prior to the maturity date of our Notes subject to certain conditions as set forth in the Credit Agreement, including the repayment of the Notes, the refinancing of the Notes including a maturity date that is at least 181 days after January 25, 2027 and compliance with a liquidity test when all amounts outstanding will be due and payable in full. If such springing maturity feature is triggered, we will be required to pay all amounts outstanding under the Credit Facility sooner than they would otherwise be due, we may not have sufficient funds available to pay such amounts at that time, and we may not be able to raise additional funds to pay such amounts on a timely basis, on terms we find acceptable, or at all.~~ The capped call transactions may affect the ~~value~~ **market price** of our common stock. In connection with the issuance of the Notes, we entered into capped call transactions with certain financial institutions (~~“~~ **"** option counterparties ~~”~~ **"**). The capped call transactions are generally expected to reduce the potential dilution to our common stock upon any conversion of the Notes and / or offset any cash payments we are required to make in excess of the principal amount of converted Notes, as the case may be, with such reduction and / or offset subject to a cap. From time to time, the option counterparties that are parties to the capped call transactions or their respective affiliates may modify their hedge positions by entering into or unwinding various derivative transactions with respect to our common stock and / or purchasing or selling our common stock or other securities of ours in secondary market transactions prior to the maturity of the Notes. This activity could cause a decrease in the market price of our common stock. The conditional conversion feature of the Notes, if triggered, may adversely affect our financial condition and operating results. Noteholders may require us to repurchase their Notes following a fundamental change at a cash repurchase price generally equal to the principal amount of the Notes to be repurchased, plus accrued and unpaid interest, if any. In addition **,** all conversions of Notes will be settled partially or entirely in cash. We may not have enough available cash or be able to obtain financing at the time we are required to repurchase the Notes or pay the cash amounts due upon conversion. In addition, applicable law, regulatory authorities and the agreements governing our other indebtedness may restrict our ability to repurchase the Notes or pay the cash amounts due upon conversion. Our failure to repurchase Notes or to pay the cash amounts due upon conversion when required will constitute a default under the indenture governing the terms of the Notes. A default under the indenture or the fundamental change itself could also lead to a default under agreements governing our other indebtedness, which may result in that other indebtedness becoming immediately payable in full. If the repayment of such other indebtedness were to be accelerated after any applicable notice or grace periods, then we may not have sufficient funds to repay that indebtedness and repurchase the Notes or make cash payments upon their conversion. We are subject to counterparty risk with respect to the capped call transactions, and the capped call may not operate as planned. The option counterparties are financial institutions, and we are subject to the risk that any or all of them might default under the capped call transactions. Our exposure

to the credit risk of the option counterparties will not be secured by any collateral. Global economic conditions have from time to time resulted in the actual or perceived failure or financial difficulties of many financial institutions. If an option counterparty becomes subject to insolvency proceedings, we will become an unsecured creditor in those proceedings with a claim equal to our exposure at that time under the capped call transactions with such option counterparty. Our exposure will depend on many factors but, generally, an increase in our exposure will be correlated to an increase in the market price subject to the cap and in the volatility of our common stock. In addition, upon a default by an option counterparty, we may suffer adverse tax consequences and more dilution than we currently anticipate with respect to our common stock. We can provide no assurances as to the financial stability or viability of the option counterparties. Provisions in the indenture could delay or prevent an otherwise beneficial takeover of us. Certain provisions in the Notes and the indenture could make a third party attempt to acquire us more difficult or expensive. For example, if a takeover constitutes a fundamental change, then Noteholders will have the right to require us to repurchase their Notes for cash. In addition, if a takeover constitutes a make- whole fundamental change, then we may be required to temporarily increase the conversion rate. In either case, and in other cases, our obligations under the Notes and the indenture could increase the cost of acquiring us or otherwise discourage a third party from acquiring us or removing incumbent management, including in a transaction that Noteholders or holders of our common stock may view as favorable. Conversion of the Notes may dilute the ownership interest of existing stockholders. The conversion of some or all of the Notes will dilute the ownership interests of existing stockholders to the extent we deliver shares of our common stock upon conversion of any of the Notes. Any sales in the public market of the common stock issuable upon such conversion could adversely affect prevailing market prices of our common stock. In addition, the existence of the Notes may encourage short selling by market participants because the conversion of the Notes could be used to satisfy short positions, or anticipated conversion of the Notes into shares of our common stock could depress the price of our common stock.