Risk Factors Comparison 2024-02-29 to 2023-03-31 Form: 10-K

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

Certain factors may have a material adverse effect on our business, financial condition, and results of operations. You should consider carefully the risks and uncertainties described below, in addition to other information contained in this Annual Report, including our consolidated financial statements and related notes. The risks and uncertainties described below are not the only ones we face. Additional risks and uncertainties that we are unaware of, or that we currently believe are not material, may also become important factors that adversely affect our business. If any of the following risks actually occurs, our business, financial condition, results of operations, and future prospects could be materially and adversely affected. In that event, the trading price of our common stock could decline, and you could lose part or all of your investment. Risks Related to Our Business Our success depends on our technology partners. In particular, our technical advantages are highly dependent on our partnership with Microsoft and other major software providers. Should Microsoft or these other providers acquire competitors that heavily overlap with our capabilities, or develop competing features, we may lose customer acquisition momentum and fail to secure renewals or growth targets. The significant majority of our customers choose to integrate their products and services with, or as an enhancement of, third- party solutions such as infrastructure, platforms or applications, in particular from Microsoft. The functionality and popularity of our products and services depend largely on our ability to integrate our platform with third- party solutions, in particular Microsoft' s Azure, SharePoint, and Office 365. We are dependent on technology partner solutions for several major categories of our offerings, including data management, migration, governance, protection and backup. As a result, our customers' satisfaction with our products are highly dependent on their perception of, and satisfaction with, our third-party providers and their respective offerings. We will continue to depend on various third- party relationships to sustain and grow our business. Third- party providers may change the features of their solutions, alter their governing terms, or end the solutions' availability altogether. They may restrict our ability to add, customize or integrate systems, functionality and customer experiences. Any such changes could limit or terminate our ability to use these third- party solutions and provide our customers with the full range of our products and services. Our business would be negatively impacted if we fail to retain these relationships for any reason, including due to third parties' failure to support or secure their technology or integrations; errors, bugs, or defects in their technology; or changes in our products and services. Any such failure, as well as a prolonged disruption, a cybersecurity event or any other negative event affecting our third- party providers and leading to customer dissatisfaction, could harm our relationship with our customers, our reputation and brand, our revenue, our business, and our results of operations. Strategic technology partners and third parties may not be successful in building integrations, co- marketing our products and services to provide significant volume and quality of lead referrals or continue to work with us as their respective products evolve. Identifying, negotiating and documenting relationships with additional strategic technology partners require significant resources. Integrating third- party technology can be complex, costly and time- consuming. Third parties may be unwilling to build integrations. We may be required to devote additional resources to develop integrations for our own products. Strategic technology partners or providers of solutions with which we have integrations may decide to compete with us or enter into arrangements with our competitors, resulting in such partners or providers withdrawing support for our integrations. Our agreements with our partners are generally non- exclusive, meaning our partners may offer products from several different companies to their customers. Specifically, Microsoft and other major platform providers could end partnerships, cease marketing our offerings, with limited or no notice and with little or no penalty, or decide to purchase strong competition, or incorporate our capabilities into native solutions. Any of these developments would negatively impact our business. Microsoft and other cloud platform providers may furthermore introduce functionality that competes with our products and services, as a result of an acquisition, or their own development. Additionally, we rely heavily on our early access to preview Microsoft technology, which enables our product strategy and development teams to anticipate future opportunities as well as validate our current direction. While Microsoft introduces competitive features as a premium option, some customers will choose a simpler first- party solution to their problem, even at a greater cost to them. Microsoft and other cloud providers may also choose to make it difficult for third party providers like us to continue making the necessary application programming interface (" API ") calls to provide their solutions, as illustrated by an increase in API " throttling " in recent years or API quotas provided by Salesforce. PART I Item 1A Although we typically receive significant advance notice of new product releases from Microsoft, Microsoft does not always preview ~~our~~ **their** technology with us or other partners and, as a result, it is possible that we may not receive advance notice of changes in features and functionality of new technologies with which our products will need to interoperate. If this was to happen, there could be an increased risk of product incompatibility. Any failure of our products and services to operate effectively with solutions could result in customer dissatisfaction and harm to our business, and could reduce the demand for our products and services. If we are unable to respond to these changes or failures in a cost- effective manner, our products and services may become less marketable, less competitive, or obsolete, and the results of our operations may be negatively impacted. We have a strategic technology partnership with Microsoft for the collaboration to co- sell and co- market our products and services to new customers. If our relationships with our strategic technology partners, such as Microsoft, are disrupted or if the co- sell and co- market program was ended for any reason, we may receive less revenue and incur costs to form other revenue- generating strategic technology partnerships. We have experienced strong growth in recent periods, and our recent growth rates may not be indicative of our future growth. We have experienced strong growth in recent periods. In future periods, we may not be able to sustain revenue growth consistent with recent history, or at all. We believe our revenue growth and our ability to manage such growth depend on several factors, including, but not limited to, our ability to do the following: ■

Effectively recruit, integrate, train and motivate a large number of new employees, including our sales force, technical solutions professionals, customer success managers and engineers, while retaining existing employees, maintaining the beneficial aspects of our corporate culture and effectively executing our business plan; ■ Attract new customers and retain and increase sales to existing customers; ■ Maintain and expand our relationships with our partners, including effectively managing existing channel partnerships and cultivating new ones; ■ Successfully implement our products and services, increase our existing customers' use of our products and services, and provide our customers with excellent customer support and the ability of our partners to do the same; ■ Develop our existing products and services and introduce new products or new functionality to our products and services; ■ Expand into new market segments and internationally; ■ Earn revenue share and customer referrals from our partner ecosystem; ■ Improve our key business applications and processes to support our business needs; ■ Enhance our internal controls to ensure timely and accurate reporting of all of our operations and financial results; ■ Protect and further develop our strategic assets, including our intellectual property rights; and ■ Make sound business decisions considering the scrutiny associated with operating as a public company. We may not accomplish any of these objectives and, as a result, it is difficult for us to forecast our future revenue or revenue growth. If our assumptions are incorrect or change in reaction to changes in our market, or if we are unable to maintain consistent revenue or revenue growth, we may not be able to maintain similar growth rates in the future. You should not rely on our revenue for any prior periods as any indication of our future revenue or revenue growth. Furthermore, these activities will require significant investments and allocation of valuable management and employee resources, and our growth will continue to place significant demands on our management and our operational and financial infrastructure. There are no guarantees we will be able to grow our business in an efficient or timely manner, or at all. Moreover, if we do not effectively manage the growth of our business and operations, the quality of our software could suffer, which could negatively affect the AvePoint brand, results of operations and overall business. Our future revenue and operating results will be harmed if we are unable to acquire new customers, expand sales to our existing customers, or develop new functionality for our products and services that achieves market acceptance. To continue to grow our business, it is important that we continue to acquire new customers to purchase and use our products and services. Our success in adding new customers depends on numerous factors, including our ability to: (1) offer compelling products and services, (2) execute our sales and marketing strategy, (3) attract, effectively train and retain new sales, marketing, professional services, and support personnel in the markets we pursue, (4) develop or expand relationships with partners, IT consultants, systems integrators resellers and other third parties, strengthening our network, (5) expand into new geographies, including internationally, and market segments, (6) efficiently onboard new customers on to our product offerings, and (7) provide additional paid services that fulfill the needs and complement the capabilities of our customers and their partners. Our future success also depends, in part, on our ability to sell additional products, more functionality and / or adjacent services to our current customers, and the success rate of such endeavors is difficult to predict ~~and~~ , especially with regard to any new products or lines of business that we may introduce from time to time. Our ability to increase sales to existing customers depends on several factors, including their experience with implementing and using our products and services, their ability to integrate our products and services with other technologies, and our pricing model. Sales to existing customers may require increasingly costly marketing and sales efforts that are targeted at senior management, and if these efforts are not successful, our business and operating results may suffer. In addition, as an increasing amount of our business may move to our cloud- based products and services and the use of consumption- based pricing models may represent a greater share of our revenue, our revenue may be less predictable or more variable than our historical revenue from perpetual or time period- based subscription pricing models. Moreover, a consumption- based subscription pricing model may ultimately result in lower total cost to our customers over time or may cause our customers to limit usage in order to stay within the limits of their existing subscriptions, reducing overall revenue or making it more difficult for us to compete in our markets. Our ability to predict the rate of customer renewals and the impact these renewals will have on our revenue or operating results is limited. Our ability to maintain or increase revenue depends in part on our ability to retain existing customers, in particular that our customers renew their subscriptions with us on the same or more favorable terms. Our customers have no obligation to renew their contracts for AvePoint products after the expiration of either the initial or renewed subscription period, and in the normal course of business, some customers elect not to renew. Our customers may renew for fewer elements of our products, for shorter renewal terms or on different pricing terms, including lower- cost offerings of our products. Our customers' renewal rates may decline or fluctuate as a result of a number of factors, including their level of satisfaction with our pricing or our products and their ability to continue their operations and spending levels, mix of customer base, decreases in the number of users at our customers, competition, pricing increases or changes, and deteriorating general economic conditions, including as a result of the **ongoing** ~~COVID- 19 pandemic or the~~ military ~~conflict~~ **conflicts** ~~between Russia and Ukraine~~ **where the outcome is not possible to predict** . If our customers do not renew their subscriptions for our products on similar pricing terms, our revenue may decline and our business could suffer. In addition, over time the average term of our contracts could change based on renewal rates or for other reasons. Further, acquisitions of our customers may lead to the cancellation of our contracts with such customers or by the acquiring companies, thereby reducing the number of our existing and potential customers. If we fail to adapt and respond effectively to rapidly changing technology, evolving industry standards, and changing customer needs or preferences, our products and services may become less competitive. The market in which we operate is characterized by the exponential growth in data generated and managed by enterprises, rapid technological advances, changes in customer requirements, including customer requirements driven by changes to legal, regulatory and self-regulatory compliance mandates, frequent new product introductions and enhancements and evolving industry standards in computer hardware and software technology. As a result, we must continually change and improve our products in response to changes in operating systems, application software, computer and communications hardware, networking software, data center architectures, programming tools and computer language technology. Moreover, the technology in our products is especially complex because it needs to effectively identify and respond to a user' s data retention, security and governance needs, while

minimizing the impact on database and file system performance. If we are unable to develop and sell new technology, features, and functionality for our products and services that satisfy our customers and that keep pace with rapid technological and industry change, our revenue and operating results could be harmed. If new technologies emerge that deliver competitive solutions at lower prices, more efficiently, more conveniently, or more securely, they could adversely impact our ability to compete. Our products and services must also integrate with a variety of network, hardware, mobile, and software platforms and technologies. We need to continuously modify and enhance our platform to adapt to changes and innovation in these technologies. If businesses widely adopt new technologies in areas covered by our products and services, we would have to develop new functionality for our products and services to work with such new technologies. This development effort may require significant engineering, marketing and sales resources, all of which would affect our business and operating results. Any failure of our products and services to operate effectively with future technologies could reduce the demand for our products and services. We cannot guarantee that it will be able to anticipate future market needs and opportunities, extend our technological expertise and develop new products or expand the functionality of our current products in a timely and cost- effective manner, or at all. Even if we can anticipate, develop and introduce new products and expand the functionality of our current products, there can be no assurance that enhancements or new products will achieve widespread market acceptance. If we fail to anticipate market requirements or stay abreast of technological changes, we may be unable to successfully introduce new products, expand the functionality of our current products or convince our existing and potential customers of the value of our products in light of new technologies. Accordingly, our business, results of operations and financial condition could be harmed. Our success with SMB customers depends in part on our resale and distribution partnerships. Our business would be harmed if we fail to maintain or expand partner relationships. We leverage the sales and referral resources of resale and referral partners through a variety of programs, and we **also** rely on distribution partners **,** especially for our SMB market acquisition. We expect that sales to partners will account for a substantial portion of our revenue for the foreseeable future. Our ability to achieve revenue growth and expand our SMB acquisition in the future will depend in part on our success in maintaining successful relationships with our partners. Our agreements with our partners are generally non- exclusive, meaning our partners may offer customers the products of several different companies. If our partners do not effectively market and sell our software, choose to use greater efforts to market and sell their own products or those of others, or fail to meet the needs of our customers, our ability to grow our business, sell our software and maintain our reputation may be harmed. Our contracts with our partners generally allow us to terminate our agreements for any reason. The loss of a substantial number of our partners, the possible inability to replace them, the failure to recruit additional partners or the removal of our products and services from several major distribution partner' s resale platforms could harm our results of operations. If we are unable to effectively utilize, maintain and expand these relationships, our revenue growth would slow, we would need to devote additional resources to the development, sales, and marketing of our products and services, and our financial results and future growth prospects would be harmed. Unfavorable conditions in our industry or the global economy, or reductions in IT spending, could limit our ability to grow our business and negatively affect our results of operations. Our results of operations may vary based on the impact of changes in our industry or the global economy on it or our customers. The revenue growth and potential profitability of our business depend on our current and prospective customers' ability and willingness to invest money in information technology services, which in turn is dependent upon their overall economic health. Current or future economic uncertainties or downturns could harm our business and results of operations. Negative conditions in the global economy or individual markets, including changes in gross domestic product growth, financial and credit market fluctuations, political turmoil, natural catastrophes, warfare and terrorist attacks on the United States, Europe, Australia, the Asia Pacific region or elsewhere, could cause a decrease in business investments, including spending on IT and negatively affect our business. Continuing uncertainty in the global economy makes it extremely difficult for us and our customers to forecast and plan future business activities accurately, and could cause our customers to reevaluate decisions to purchase our products and services or to delay their purchasing decisions, which could lengthen our sales cycles. To the extent our products and services are perceived by our existing and potential customers as costly, or too difficult to launch or migrate to, it would negatively affect our growth. Our revenue may be disproportionately affected by delays or reductions in general IT spending. Competitors may respond to market conditions by lowering prices and attempting to lure away our customers. In addition, consolidation in certain industries may result in reduced overall spending on our products and services. We have a significant number of customers in the financial services, the public sector and the pharmaceutical and manufacturing industries. A substantial downturn in any of these industries, or a reduction in public sector spending, may cause enterprises to react to worsening conditions by reducing their capital expenditures in general or by specifically reducing their spending on information technology. Customers may delay or cancel information technology projects, choose to focus on in- house development efforts or seek to lower their costs by renegotiating maintenance and support agreements. To the extent purchases of licenses for our software are perceived by our existing and potential customers to be discretionary, our revenue may be disproportionately affected by delays or reductions in general information technology spending. We cannot predict the timing, strength, or duration of any economic slowdown, instability or recovery, generally or within any particular industry. If the economic conditions of the general economy or markets in which we operate worsen from present levels, our business, results of operations and financial condition could be harmed. Failure to effectively develop and expand our marketing and sales capabilities could harm our ability to increase our customer base and achieve broader market acceptance of our products and services. If we are not able to generate traffic to our website through digital marketing, our ability to attract new customers may be impaired. Our ability to increase our customer base and achieve broader market acceptance of our products and services will depend on our ability to expand our marketing and sales operations. We plan to continue expanding our sales force and strategic partners, both domestically and internationally. We also have dedicated, and plans to further dedicate, significant resources to sales and marketing programs, including search engine and other online advertising. The effectiveness of our online advertising may continue to vary due to competition for key search terms, changes in search engine use, and changes in search algorithms

used by major search engines and other digital marketing platforms. Another major investment is in marketing technology to better connect our systems and data among sales, product, and marketing, in order to create a more seamless user experience. Our business and operating results will be harmed if our sales and marketing efforts do not generate a corresponding increase in revenue. We may not achieve anticipated revenue growth from expanding our sales force if we are unable to hire, develop, and retain talented sales personnel, if our new sales personnel are unable to achieve desired productivity levels in a reasonable period of time, or if our sales and marketing programs are not effective. If the cost of marketing our products and services over search engines or other digital marketing platforms increases, our business and operating results could be harmed. Competitors also may bid on the search terms that we use to drive traffic to our website. Such actions could increase our marketing costs and result in decreased traffic to our website. Furthermore, search engines and digital marketing platforms may change their advertising policies from time to time. If these policies delay or prevent us from advertising through these channels, it could result in reduced traffic to our website and subscriptions to our products and services. New search engines and other digital marketing platforms may develop, particularly in certain jurisdictions, that reduce traffic on existing search engines and digital marketing platforms. If we are not able to achieve prominence through advertising or otherwise, it may not achieve significant traffic to our website through these new platforms and our business and operating results could be harmed. We depend on third-party data hosting and transmission services. Increases in cost, interruptions in service, latency, or poor service from our third-party data center providers could impair the delivery of our platform. This could result in customer dissatisfaction, damage to our reputation, loss of customers, limited growth, and reduction in revenue. We currently serve the majority of our SaaS offerings from third- party data center hosting facilities in different geographical locations that are operated by Microsoft. Our products and services, in particular SaaS offerings, are deployed to multiple data centers within these geographies, with additional geographies available for disaster recovery. Our operations depend, in part, on our third- party providers' protection of these facilities from natural disasters, power or telecommunications failures, criminal acts, or similar events. If any third-party facility' s arrangement is terminated, or our service lapses, we could experience interruptions in our platform, latency, as well as delays and additional expenses in arranging new facilities and services. A significant portion of our operating costs are from our third- party data hosting and transmission services. If the costs for such services increase due to vendor consolidation, regulation, contract renegotiation or otherwise, we may not be able to increase the fees for our products and services to cover the changes. As a result, our operating results may be significantly worse than forecasted. Our failure to achieve or maintain sufficient and performant data transmission capacity could significantly reduce demand for our products and services. Seasonal or singular events may significantly increase the traffic on our own and the used third- party' s servers and the usage volume of our products. Despite precautions taken at the used data centers, spikes in usage volume, a natural disaster, an act of terrorism, vandalism or sabotage, closure of a facility without adequate notice, or other unanticipated problems (such as the military conflict between Russia and Ukraine) could result in lengthy interruptions or performance degradation of our platform. Our own and third party data centers may also be subject to national or local administrative actions, changes in government regulations, including, for example, the impact of global economic and other sanctions like those levied in response to the Russia- Ukraine crisis, changes to legal or permitting requirements and litigation to stop, limit or delay operations. Any damage to, or failure of, the systems of our third- party providers could result in interruptions to our products and services. Even with current and planned disaster recovery arrangements, our business could be harmed. If we experience damage or interruption, our insurance policies may not adequately compensate us for any losses that we may incur. These factors in turn could further reduce our revenue, subject us to liability, cause us to issue credits, or cause customers to terminate their subscriptions, any of which could harm our business. If we incur such losses or liabilities, we might be unable to recover significant amounts from our third- party providers (even if they were primarily or solely responsible) because of restrictive liability and indemnification terms. If there are interruptions or performance problems associated with our technology or infrastructure, our existing customers may experience service outages, and our new customers may experience delays in using our products and services. Our continued growth depends, in part, on the ability of our existing and potential customers to access our products and services 24 hours a day, seven days a week, without interruption or performance degradation. We have experienced, and may in the future experience, disruptions, outages, and other performance problems with our infrastructure. These can be due to a variety of factors, including infrastructure changes, introductions of new functionality, human or software errors, capacity constraints, denial- of- service attacks, or other security- related incidents, any of which may be recurring. As we continue to add customers, expand geographically, and enhance our products' and / or services' functionality, the additional scale may increase complexity and our average uptime for future periods may decrease. We may not be able to identify the cause or causes of these performance problems promptly. If our products and services are unavailable or if our customers are unable to access our products and services within a reasonable amount of time, our business would be harmed. Any outage of our products and services would impair the ability of our customers to engage in their own business operations, which would negatively impact our brand, reputation and customer satisfaction. We provide service credits to our customers for downtime they experience using our SaaS products. Any downtime or malfunction could require us to issue a significant amount of service credits to customers. Issuing a significant amount of service credits would negatively impact our financial position. We depend on services from various third parties to maintain our infrastructure and any disruptions to these services, including from causes outside our control, would significantly impact our products and services. In the future, these services may not be available to us on commercially reasonable terms, or at all. Loss of any of these services could decrease our products' and / or services' functionality until we develop equivalent technology or, if equivalent technology is available from another party, we identify, obtain and integrate it into our infrastructure. If we do not accurately predict our infrastructure capacity requirements, our customers could experience service shortfalls. We may also be unable to address capacity constraints, upgrade our systems, and develop our technology and network architecture to accommodate actual and anticipated technology changes. Any of the above circumstances or events may harm our reputation, cause customers to terminate their agreements with us, impair our ability to

grow our customer base, subject us to financial liabilities, and otherwise harm our business, results of operations, and financial condition. Risks Related to Our Operations and Financial Condition Our operations will continue to increase in complexity as we grow, which will create management challenges. Our business has experienced strong growth and is complex. This growth is expected to continue, and our operations will be increasingly complex. To manage this growth, we will make substantial investments to improve our operational, financial, and management controls as well as our reporting systems and procedures. We may not be able to implement and scale improvements to our systems and processes in a timely or efficient manner or in a manner that does not negatively affect our operating results. For example, we may not be able to effectively monitor certain extraordinary contract requirements or individually negotiated provisions as the number of customers continues to grow. Our systems and processes may not prevent or detect all errors, omissions, or fraud. We may have difficulty managing improvements to our systems, processes and controls or in connection with third- party software. This could impair our ability to provide our products and services to our customers, causing us to lose customers, limiting products and services to less significant updates, or increasing technical support costs. If we are unable to manage this complexity, our business, operations, operating results and financial condition may suffer. As our customer base continues to grow, we will need to expand our services and other personnel and maintain and enhance our partnerships to provide a high level of customer service ~~. Extended stay- at- home, business closure, and other restrictive orders may impact our ability to identify, hire, and train new personnel~~ . We will also need to manage our sales processes as our sales personnel and partner network continue to grow and become more complex, and as we continue to expand into new geographies and market segments. If we do not effectively manage this increasing complexity, the quality of our platform and customer service could suffer, and we may not be able to adequately address competitive challenges. These factors could impair the ability to attract and retain customers and expand customers' use of our products and services. If we fail to maintain or grow our brand recognition, our ability to expand our customer base will be impaired and our financial condition may suffer. We believe enhancing the AvePoint brand and maintaining our reputation in the information technology industry will be critical for the continued acceptance of our existing and future products and services, attracting new customers to our products and services, and retaining existing customers. The importance of brand recognition will increase as competition in our market increases. Successfully maintaining our brand will depend largely on the effectiveness of our marketing efforts, the ability to provide high- quality, innovative, reliable and useful products and services to meet the needs of our customers at competitive prices, the ability to be responsive to customer concerns and provide high quality customer support, training and professional services, the ability to maintain our customers' trust, the ability to continue to develop new functionality and products, and the ability to successfully differentiate our products and services. Additionally, partners' performance may affect the AvePoint brand and reputation if customers do not have a positive experience. Brand promotion activities may not generate customer awareness or yield increased revenue. Even if they do, any increased revenue may not offset the expenses incurred in building our brand. Furthermore, independent industry analysts may provide reviews of our products and services, as well as other products available in the market, and perception of our products and services in the marketplace may be significantly influenced by these reviews. If these reviews are negative, or less positive than reviews about other products available in the market, the AvePoint brand may be harmed. Furthermore, negative publicity relating to events or activities attributed to employees, partners or others associated with any of these parties, may tarnish our reputation and reduce the value of our brand. Damage to reputation and loss of brand equity may reduce demand for our products and harm our business, results of operations and financial condition. Any attempts to rebuild our reputation and restore the value of our brand may be costly and time consuming, and such efforts may not ultimately be successful. If we fail to successfully promote and maintain our brand, we may fail to attract enough new customers or retain existing customers to realize a sufficient return on our brand- building efforts, and our business could suffer. If we fail to offer high quality support, our business and reputation could suffer. Our customers have historically relied on our personnel for support related to our products, in particular SaaS products. High- quality support will continue to be important for the renewal and expansion of agreements with our existing customers. The importance of high-quality support will increase as we expand our business and pursue new customers. If we do not help our customers quickly resolve issues and provide effective ongoing support, our ability to sell new products and services to existing and new customers could suffer and our reputation with existing or potential customers could be harmed. If our products and services do not effectively interoperate with our customers' existing or future IT infrastructures or do not operate as effectively when accessed through mobile devices, customers may not be satisfied, which could harm our business. Our success will depend in part on the interoperability of our products and services with third- party operating systems, applications, data, web browsers and devices that hawse have not developed and does not control. Due to the continuing rapid growth of the use of mobile devices in business operations, this also includes third- party mobile devices and mobile operating systems. Any changes in such operating systems, applications, data, web browsers or devices that degrade the functionality of our products and services or give preferential treatment to competitive services could harm the adoption and usage of our products and services. We may not be successful in adapting our products and services to operate effectively with these operating systems, applications, data or devices. Effective mobile functionality is a part of our long- term development and growth strategy. If customers have difficulty accessing and using our products and services (including on mobile devices) or if our products and services cannot connect a broadening range of applications, data and devices, then customer growth and retention may be harmed and our business and operating results could be harmed. Being a global company may create a variety of operational challenges. Our international operations will involve a variety of risks, including: ■ Changes in a country' s or region' s political or economic conditions; ■ Economic uncertainty around the world and adverse effects arising from economic interdependencies across countries and regions; ■ The need to adapt and localize products and services for specific countries; ■ Greater difficulty in receiving payments from different geographies, including difficulties associated with currency fluctuations, transfer of funds, longer payment cycles and collecting accounts receivable, especially in emerging markets; ■ Potential changes in trade relations arising from policy initiatives implemented by the current administration or by a successor administration; ■ Compliance with foreign laws and regulations

and the risks and costs of non- compliance with such laws and regulations; ■ Unexpected changes in laws, regulatory requirements, taxes, or trade laws; ■ More stringent regulations relating to privacy and data security and the unauthorized use of, or access to, commercial and personal information, particularly in Europe; ■ Differing labor regulations, especially in Europe, where labor laws are generally more advantageous to employees as compared to the United States, including deemed hourly wage and overtime regulations in these locations; ■ Challenges inherent in efficiently managing an increased number of employees over large geographic distances (including in a work- from- home environment), including the need to implement appropriate systems, policies, benefits, and compliance programs; ■ Difficulties in managing a business in new markets with diverse cultures, languages, customs, legal systems, alternative dispute systems, and regulatory systems; ■ Increased travel, real estate, infrastructure, and legal compliance costs associated with international operations; ■ Currency exchange rate fluctuations and the resulting effect on revenue and expenses, and the cost and risk of entering into hedging transactions if we elect to do so in the future; ■ Limitations on the ability to reinvest earnings from operations in one country to fund the capital needs of our operations in other countries; ■ Laws and business practices favoring local competitors or general preferences for local vendors; ■ limited or insufficient intellectual property protection or difficulties enforcing our intellectual property; ■ Political instability or terrorist activities; ■ Exposure to liabilities under anti- corruption and anti- money laundering laws, including the U. S. Foreign Corrupt Practices Act of 1977, as amended (the " FCPA "), the U. S. domestic bribery statute contained in 18 U. S. C. § 201, the U. S. Travel Act, the UK Bribery Act of 2010, the UK Proceeds of Crime Act 2002, and similar laws and regulations in other jurisdictions; ■ Compliance with laws and regulations for foreign operations, import and export control laws, tariffs, trade barriers, economic sanctions and other regulatory or contractual limitations on the ability to sell our software in certain foreign 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 financial results and result in restatements of financial statements and irregularities in financial statements; and ■ Adverse tax burdens and foreign exchange controls that could make it difficult to repatriate earnings and cash. In addition, certain of our customer or resellers may operate in, or have dealings with, countries subject to sanctions or embargos imposed by the U. S. government, foreign governments, or the United Nations or other international organizations. **These** ~~In particular, on February 24, 2022, Russian troops began a full- scale invasion of Ukraine and, as of the date hereof, the countries remain in active armed conflict. Around the same time, the U. S., the U. K., the E. U., and several other nations announced a broad array of new or expanded~~ sanctions ~~, export controls, and~~ **or embargos may result from** ~~other~~ -- **the multiple ongoing conflicts where** ~~measures against Russia, Russian- backed separatist regions in Ukraine, and certain banks, companies, government officials, and other~~ -- **the outcomes** ~~individuals in Russia~~ and ~~Belarus~~ **consequences are not possible to predict** , **but** ~~as well as a number of Russian Oligarchs. The U. S. or other countries~~ could **include regional instability** ~~also institute broader sanctions on Russia~~ and ~~others supporting Russia' s~~ **geopolitical shifts, and could materially adversely affect global trade, currency exchange rates, regional economies and the global** economy ~~or military efforts~~ . ~~The~~ **These** ~~ongoing conflict~~ **conflicts** and **any actions taken** ~~the rapidly evolving measures~~ in response could ~~be expected~~ **increase our costs, disrupt our supply chain, reduce our sales and earnings, impair our ability** to ~~have a negative impact~~ **raise additional capital when needed** on **acceptable terms** ~~the economy and business activity globally (including in the countries in which the Company invests)~~ , **if at all, or otherwise** ~~and therefore are expected to result in adverse~~ **adversely** ~~consequences to the Russian economy and could have a material adverse effect~~ **affect** ~~on~~ our business, financial condition, ~~cash flows~~ and results of operations. ~~The~~ **These** ~~severity and duration of the conflict~~ **conflicts** and ~~its impact on global economic and market conditions are impossible to predict, and as a result, present material uncertainty and risk with respect to our operations, and our ability to achieve our objectives. Similar risks will exist to the extent that~~ any ~~service providers, vendors or certain other parties have material operations or assets in Russia, Ukraine, Belarus, or the immediate surrounding areas. Sanctions~~ -- **actions taken in response** could also result in ~~Russia taking counter measures~~ **the aforementioned impacts on the business of** ~~or~~ **our** ~~retaliatory actions~~ **customers, resellers or any other service providers on** which **we** ~~could adversely impact our business or the business of our partners, including, but not limited to, cyberattacks targeting private companies, individuals or other infrastructure upon which our business and the business of our partners may~~ rely. Any of these risks could harm our international operations, reduce our revenue from outside the United States or increase our operating costs, harming our business, results of operations and financial condition and growth prospects. There can be no assurance that all of our employees, independent contractors and partners will comply with the formal policies we will implement, or applicable laws and regulations. Violations of laws or key control policies by employees, independent contractors and partners could result in delays in revenue recognition, financial reporting misstatements, fines, penalties or the prohibition of the importation or exportation of our software and services and could harm our business and results of operations. If we invest substantial time and resources to expand our international operations and is unable to do so successfully, our business and operating results will suffer. We are exposed to fluctuations in currency exchange rates, which could negatively our revenue and earnings. We conduct a significant number of transactions and hold cash in currencies other than the U. S. Dollar. Changes in the values of major foreign currencies relative to the U. S. Dollar may significantly affect our total assets, revenue, operating results and cash flows, which are reported in U. S. Dollars. We may acquire or invest in companies, which may divert management' s attention and result in additional dilution to stockholders. We may be unable to integrate acquired businesses and technologies successfully or achieve the expected benefits of such acquisitions. We may evaluate and consider potential strategic transactions, including acquisitions of, or investments in, businesses, technologies, services, products, and other assets in the future. An 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. Key personnel of the acquired companies may choose not to work for us, their software may not be easily adapted, or we may have difficulty retaining the customers of any acquired business due to changes in ownership, management, or otherwise. We may also experience difficulties integrating personnel of the acquired

company into our business and culture. Acquisitions may also disrupt our business, divert our resources and require significant management attention that would otherwise be available for development of our existing business. The anticipated benefits of any acquisition, investment, or business relationship may not be realized or we may be exposed to unknown risks or liabilities. We intend to continue investing in research and development, and to the extent such research and development investments do not translate into new products or material enhancements to our products, or if we do not use those investments efficiently, our business and results of operations would be harmed. A key element of our strategy will be to invest significantly in our research and development efforts to develop new products and enhance our existing products to address additional applications and markets. If we do not spend our research and development budget efficiently or effectively on compelling innovation and technologies, 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 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 products and generate revenue, if any, from such investment. Additionally, anticipated customer demand for a product or service being developed 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 product or service. 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 products that are competitive in our current or future markets, it would harm our business and results of operations. If our products and services fail to perform properly, or if we fail to develop enhancements to resolve performance issues, we could lose customers, become subject to performance or warranty claims, or incur significant costs. Our operations will be dependent upon our ability to prevent system interruption. The applications underlying our products and services are inherently complex and may contain material defects or errors, which may cause disruptions in availability or other performance problems. Also, our software will be installed and used in a variety of computing environments with different operating system management software, and equipment and networking configurations, which may cause errors or failures of our software or other aspects of the computing environment into which it is deployed. In addition, deployment of our software into computing environments may expose undetected errors, compatibility issues, failures or bugs in our software. While we have not historically experienced any defects, errors, disruptions in service, cyber- attacks, or other performance problems with our software that materially influenced our sales performance, there is no assurance that such defects, problems or events will not occur in the future, whether in connection with the day- to- day operation, upgrades or otherwise. Any of these occurrences could result in loss of customers, lost or delayed market acceptance and sales of our products and services, delays in payment by customers, injury to our reputation and brand, legal claims, including warranty and service claims, diversion of resources, including through increased service and warranty expenses or financial concessions, and increased insurance costs. We may discover defects in our products and services that could result in data unavailability, unauthorized access, loss, corruption, or other harm to our customers' data. Despite testing we may not be able to detect and correct defects or errors before release. Consequently, we or our customers may discover defects or errors after our products and services have been deployed. We expect to implement bug fixes and upgrades as part of our regularly scheduled system maintenance. If we do not complete this maintenance according to schedule or if customers are otherwise dissatisfied with the frequency and / or duration of our maintenance services and related system outages, customers could terminate their contracts, delay or withhold payment, or cause us to issue credits, make refunds, or pay penalties. The costs incurred or delays resulting from the correction of defects or errors in our software or other performance problems may be substantial and could harm our operating results. Moreover, customers could incorrectly implement or inadvertently misuse our software, which could result in customer dissatisfaction and adversely impact the perceived utility of our products as well as our brand. Any of these real or perceived errors, compatibility issues, failures or bugs in our software could result in negative publicity, reputational harm, loss of or delay in market acceptance, loss of competitive position or claims by customers for losses sustained by them. In such an event, we may be required, or may choose, for customer relations or other reasons, to expend additional resources in order to help correct the problem. Risks Related to Data Privacy and Cybersecurity To the extent our security measures are compromised, our products and services may be perceived as not being secure. This may result in customers curtailing or ceasing their use of our products and services, our reputation being harmed, the incurrence of significant liabilities, and harm to our results of operations and growth prospects. Our operations may, in some cases, involve the storage, transmission and other processing of customer data or information. Cyberattacks and other malicious internet- based activity continue to increase, and cloud- based platform providers of services are expected to continue to be targeted. Threats include traditional computer " hackers, " malicious code (such as viruses and worms), phishing attacks, employee theft or misuse and denial- of- service attacks. Sophisticated nation- states and nation- state supported actors now engage in such attacks, including advanced persistent threat intrusions. The growth in state sponsored cyber activity, including the increased rate of cyberattacks arising from the Russia- Ukraine crisis and the risk that these cyberattacks could spread globally, showcases the increasing sophistication of cyber threats and could dramatically expand the global threat landscape. While no single company can thwart a nation state attack, we work to implement and continuously improve security- aware software development, operational management, and threat- mitigation practices that are essential to the strong protection of services and data. AvePoint has decades- long experience building enterprise software and running online services around the world. We implement a robust defense- in- depth security strategy based on the principle of " assume breach. " We work to continuously strengthen threat detection, response, and defense, conduct continuous security monitoring, and practice security incident response to validate and improve the security of our software and services. Rigorous third- party audits verify that we adhere to strict security controls such as the ones contained in the ISO / IEC 27001 standard mandate. We are audited once a year for ISO / IEC 27001 **, 27017 and 27701** compliance by a third- party accredited certification body, which provides independent validation that security controls are in place and operating effectively. We have security measures in place designed to protect us and our customers' confidential and sensitive information and prevent data loss, but such

measures cannot provide absolute security and may not be effective to prevent a security breach, including as a result of employee error, theft, misuse or malfeasance, third- party actions, unintentional events or deliberate attacks by cyber criminals, any of which may result in someone obtaining unauthorized access to our customers' data, our data, our intellectual property and / or other confidential or sensitive business information. Importantly, the scope of our internal information controls and security measures is limited to the scope of our information security management system (" ISMS "). All of the legal entities (and each of their respective employees) within our global corporate structure are contractually bound to the ISMS, but failure by any of our subsidiaries or affiliates (or employees thereof) to abide by the terms and conditions imposed by our ISMS could result in increased vulnerabilities, decreased integrity of our assets, and ultimately, liability, loss of business, and loss of customer confidence. The ISMS applies to the use of information, network resources, and electronic and computing devices to conduct business or interact with internal networks and business systems, whether owned or leased by us, our employees, or a third party. All employees, contractors, consultants, as well as our affiliates and subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the ISMS, as well as local laws and regulation. While we have policies and procedures to address global compliance with the ISMS, our employees and agents could violate these policies and applicable law, for which we may be ultimately held responsible. We are taking further steps to assess globally managed departmental systems to ensure ISMS standards are maintained. Based on the results of that analysis, if, as, and when necessary, we will subsequently implement a remediation plan that will include tools, training, and education to ensure (A) repeatable procedures are being implemented that protect the confidentiality, availability, and integrity of assets from threats and vulnerabilities in accordance with the ISMA standards and protocols, and (B) that vulnerability testing is being performed, measured, and documented across our global operations landscape. Outside of the ISMS and the internal security measures and data protections we have developed (and continue to improve), third parties may attempt to fraudulently induce employees, contractors or users to disclose information, including user names and passwords, to gain access to our customers' data, our data or other confidential or sensitive information, and we may be the target of email scams that attempt to acquire personal information or our assets. Because techniques used to sabotage or obtain unauthorized access to systems change frequently and generally are not recognized until successfully launched against a target, we may be unable to anticipate these techniques, react in a timely manner or implement adequate preventative measures. We devote significant financial and personnel resources to implement and maintain security measures; however, such resources may not be sufficient, and as cyber- security threats develop, evolve and grow more complex over time, it may be necessary to make significant further investments to protect our data and infrastructure. If our security measures are compromised as a result of third- party action, employee or customer error, malfeasance, stolen or fraudulently obtained log- in credentials, or otherwise, our reputation and business could be damaged and we could incur significant liability. As we rely on third- party and public-cloud infrastructure, it depends in part on third- party security measures to protect against unauthorized access, cyberattacks, and the mishandling of customer data. A cybersecurity event could have significant costs, including regulatory enforcement actions, litigation, litigation indemnity obligations, remediation costs, network downtime, increases in insurance premiums, and reputational damage. ~~Many companies that provide cloud- based services have reported a significant increase in cyberattack activity since the beginning of the COVID- 19 pandemic. T- hese~~ **These** risks, as well as the number and frequency of cybersecurity events globally, may also be heightened during times of geopolitical tension or instability between countries, including, for example, the ongoing military conflict between Russia and Ukraine, from which a number of recent cybersecurity events have been alleged to have originated. We store confidential company information and sensitive data, including personal information of our customers and employees, which may in turn contain third- party personal or other confidential information. If the security of this information is compromised or is otherwise accessed without authorization, our reputation may be harmed, and we may be exposed to liability and loss of business. We may in some cases transmit or store personal and other confidential information of our partners, customers, and third parties (e. g. if the customer uses our products to create backups of their information) on storage space owned or provided by us. While we have in the past taken, and intend to take, steps to protect personal information and other confidential information that we have access to, including information we may obtain through our customer support services or customer usage of our products, we will not proactively monitor (or may not even be able to access) the content that our customers upload or process otherwise or the information provided to us through the use of our products and services. Therefore, we will not control the substance of the content on our storage space owned or provided by us, which may include personal or other confidential information. We will also use third- party service providers and sub-processors to help us deliver services to our customers. Such service providers and sub- processors may store personal information and / or other confidential information. Such information may be the target of unauthorized access or subject to security breaches as a result of third- party action, **exploitation of artificial intelligence,** employee error, malfeasance or otherwise ~~. Many companies that provide these services have reported a significant increase in cyberattack activity since the beginning of the COVID- 19 pandemic~~ . Any of these could result in the loss of information, litigation, indemnity obligations, damage to our reputation and other liability or harm our business, financial condition, and results of operations. Because the techniques used to obtain unauthorized access or sabotage systems change frequently and generally are not identified until they are launched against a target, we may be unable to anticipate these techniques or to implement adequate preventative measures. Even if such a data breach did not arise out of our action or inaction, or if it were to affect one or more of our competitors or customers' competitors, rather than us, the resulting concern could negatively affect our customers and our business. Concerns regarding data privacy and security may cause some customers to stop using our products and services and fail to renew their subscriptions. In addition, failures to meet our customers' expectations with respect to security and confidentiality of their data and information could damage our reputation and affect our ability to retain customers, attract new customers, and grow our business. Our potential failure to comply with legal or contractual requirements around the security of personal information could lead to significant fines and penalties, as well as claims by customers, affected data subjects, or other stakeholders. These

proceedings or violations could force us to spend money in defense or settlement of these proceedings, result in the imposition of monetary liability or injunctive relief, divert management' s time and attention, increase our costs of doing business, and harm our reputation and the demand for our platform. If credit card information is stored in our systems or transmitted, stored or otherwise processed via our products and services and our security measures fail to protect credit card information adequately, we could be liable to our partners, the payment card associations, our customers or affected credit card holders. We could be subject to fines and face regulatory or other legal action, and our customers could end their relationships with us. The limitations of liability in our contracts may not be enforceable or adequate or would otherwise protect us from any such liabilities or damages with respect to any particular claim. Insurers could deny coverage as to any future claim. We seek to cap the liability to which we are exposed in the event of losses or harm to our customers, including those resulting from security incidents, but we cannot be certain that we will obtain these caps or that these caps, if obtained, will be enforced in all instances. The successful assertion of one or more large claims against us, or changes in insurance policies, including premium increases or the imposition of large deductible or co- insurance requirements, could harm our business, financial condition, and results of operations. Furthermore, the cybersecurity insurance we maintain may be inadequate or may not be available in the future on acceptable terms, or at all. In addition, our policy may not cover our remediation expenses or any claim against us for loss of data or other indirect or consequential damages. Defending any suit based on or related to any data loss or system disruption, regardless of its merit and available insurance coverage, could be costly and divert management' s attention. We will also be subject to federal, state, and foreign laws regarding cybersecurity and the protection of data. Many jurisdictions have enacted laws requiring companies to notify individuals of security breaches involving certain types of personal information. Our agreements with certain customers and partners will require us to notify them of certain security incidents. Some jurisdictions and customers require us to safeguard personal information or confidential information using specific measures. If we fail to observe these requirements, our business, operating results, and financial condition could be harmed. Successful cyberattacks or data breaches at other technology companies, service providers, retailers, and other participants within our industry, whether or not we are impacted, could lead to a general loss of customer confidence that could negatively affect us, including harming the market perception of the effectiveness of our security measures, which could result in reduced use of our products and services. Our industry is prone to cyber- attacks by third parties seeking unauthorized access to our data or users ' data or to disrupt our and our counterparts' within the industry respective ability to provide service. Our products and services (and those of our partners and competitors within the industry) involve the collection, storage, processing, and transmission of a large amount of data. Any failure by those institutions and participants in our industry to prevent or mitigate security breaches and improper access to or disclosure of data or user data, including personal information, content, or payment information from users, or information from marketers, could result in the loss, modification, disclosure, destruction, or other misuse of such data, which could indirectly harm our business and reputation and diminish our competitive position within the market generally. In addition, computer malware, viruses, social engineering (such as spear phishing attacks), scraping, and general hacking continue to be prevalent in our industry, and while we anticipate that such events may occur on our systems in the future, the impact on those within our industry has already adversely impacted the market' s perception of the effectiveness of our and our partners' security measures and countermeasures. Such breaches and attacks on our counterparts within the industry and within our market may cause, among other things, interruptions to the provision of service, degradation of the user experience, the loss of user confidence and trust in our products, or result in financial harm to us. Risks Related to Intellectual Property We will rely on third- party proprietary and open source software for our products and services. The inability to obtain third- party licenses for such software, obtain them on favorable terms, or adhere to the license terms for such software or any errors or failures caused by such software could harm our business, results of operations and financial condition. Some of our offerings will include software or other intellectual property licensed from third parties. It may be necessary in the future to renew licenses relating to various aspects of these applications or to seek new licenses for existing or new applications. Necessary licenses may not be available on acceptable terms or under open source licenses permitting redistribution in commercial offerings, if at all. The inability to obtain certain licenses or other rights or to obtain such licenses or rights on favorable terms could result in delays in product releases until equivalent technology can be identified, licensed or developed, if at all, and integrated into our products and services, which could harm our business, results of operations and financial condition. Third parties may allege that additional licenses are required for our use of their software or intellectual property, which it may be unable to obtain on commercially reasonable terms or at all. The inclusion in our offerings of software or other intellectual property licensed from third parties on a non- exclusive basis could limit our ability to differentiate our offerings from those of our competitors. Failure to properly adhere to the license terms for software or other intellectual property might have negative effects, such as revocation of the license grant, penalties, added license fees or other liabilities. To the extent that our products and services depend upon the successful operation of third- party software, any undetected errors or defects in such third- party software could impair the functionality of our products and services, delay new feature introductions, result in a failure of products and services, and injure our reputation. A significant portion of our products will incorporate open source software, and we expect to incorporate open source software into other offerings or products in the future. Such open source software is generally licensed by its authors or other third parties under open source licenses. Little legal precedent governs the interpretation of these licenses; therefore, the potential impact of these terms on our business is unknown and may result in unanticipated obligations regarding our technologies. If a distributor of open source software were to allege that we had not complied with our license, we could be required to incur significant legal expenses. In addition, if the license terms for the open source code change we may be forced to re- engineer our software or incur additional costs. If we combine our proprietary software with open source software or utilizes open source software in a certain manner, under some open source licenses, we could be in breach of the license if we did not release the source code of our proprietary software. Releasing the source code could substantially help competitors develop products that are similar to or better than ours and could help malevolent actors detect security weaknesses to develop

and deploy attacks, including malware, against our products and systems. If we are unable to protect our intellectual property, the value of our brands and other intangible assets may be diminished, and our business may be adversely affected. We rely and expect to continue to rely on a combination of confidentiality, assignment, and license agreements with our employees, consultants, and third parties with whom we have relationships, as well as trademark, copyright, patent, trade secret, and domain name protection laws, to protect our proprietary rights. Third parties may knowingly or unknowingly infringe our proprietary rights, third parties may challenge proprietary rights held by us, and pending and future trademark and patent applications may not be approved. In addition, effective intellectual property protection may not be available in every country in which we operate or intend to operate our business. In any or all of these cases, we may be required to expend significant time and expense in order to prevent infringement or to enforce our rights. Although we have generally taken measures to protect our proprietary rights, there can be no assurance that others will not offer products or concepts that are substantially similar to ours and compete with our business. **Risks Related to Financial Reporting** Our management has identified material weaknesses in our internal control over financial reporting and we may identify additional material weaknesses in the future or otherwise fail to maintain an effective system of internal controls, which may result in material misstatements of our financial statements or cause us to fail to meet our periodic reporting obligations. ~~As~~ **We are** a public company, **and** our management is required to maintain internal control over financial reporting and to report any material weaknesses in such internal control. Prior to the consummation of the **Apex** Business Combination, we were a private company with limited accounting and financial reporting personnel and other resources with which to address our internal controls and procedures. A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting such that there is a reasonable possibility that a material misstatement of our annual or interim financial statements will not be prevented or detected on a timely basis. We determined that we had material weaknesses in ~~internal~~ **the design and implementation of** control **activities** ~~because we did not maintain effective controls related~~ to **address** ~~: (i)~~ the completeness and accuracy of **certain information relevant for control owners to perform their control activities over** financial accounting, reporting and disclosures ~~, (ii) the identification, review and accounting for nonroutine transactions and / or events and (iii) segregation of duties with respect to the processing of financial transactions~~ . With the oversight of senior management and our audit committee, we implemented actions under a remediation plan which include (A) **enhancement** ~~the hiring~~ of **the design** ~~personnel with technical accounting and financial reporting experience to further bolster our ability to assess judgmental areas~~ of ~~accounting and provide~~ **controls that address the completeness** ~~an~~ **and accuracy** ~~appropriate level~~ of ~~oversight~~ **reports being utilized in the execution** of ~~activities related to~~ internal ~~control~~ **controls** ~~over financial reporting~~ and (B) ~~the engagement~~ **continuous evaluation** of ~~external consultants in~~ the **assignment of responsibilities associated with the performance of control activities and consider hiring additional resources, obtaining third party** assistance **, and providing** ~~of the evaluation of complex accounting matters. We are implementing~~ additional **training** ~~actions under a remediation plan which include, but are not limited~~ to **existing resources** ~~, (I) the implementation of improved accounting and financial reporting procedures and controls to improve the completeness and accuracy of our financial accounting, reporting and disclosures and (II) the establishment of formalized internal controls to review and maintain segregation of duties between control operators~~ . We have continued the implementation of this plan and believe the measures described above will remediate the material weaknesses identified and strengthen our internal control over financial reporting. We are committed to continuing to improve our internal control processes and will continue to diligently and vigorously review our financial reporting controls and procedures. While we continue to implement our plan to remediate the material weaknesses described above, we cannot predict the success of such plan or the outcome of our assessment of these plans at this time. If our steps are insufficient to remediate the material weaknesses successfully and otherwise establish and maintain an effective system of internal control over financial reporting, the reliability of our financial reporting, investor confidence in us, and the value of our common stock could be materially and adversely affected. We can give no assurance that the implementation of this plan will remediate these deficiencies in internal control or that additional material weaknesses or significant deficiencies in our internal control over financial reporting will not be identified in the future. Our failure to implement and maintain effective internal control over financial reporting could result in errors in our financial statements that could result in a restatement of our financial statements, causing us to fail to meet our reporting obligations. As a public company, we are obligated to develop and maintain proper and effective internal control over financial reporting in order to comply with Section 404 of the Sarbanes-Oxley Act. We may not complete our analysis of our internal control over financial reporting in a timely manner, these internal controls may not be determined to be effective, and our independent registered public accounting firm may issue an adverse opinion, which may adversely affect investor confidence in us and, as a result, the value of our common stock. Our management is responsible for establishing and maintaining adequate internal control over financial reporting. Internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements in accordance with GAAP. We **aim** ~~are in the very early stages of the costly and challenging process of compiling the system and processing documentation necessary~~ to **comply with and** perform the ~~evaluation~~ **evaluations** needed to comply with Section 404 of the Sarbanes- Oxley Act (" SOX "). In addition to our remediation efforts described **in the previous risk factor** under the heading " ~~our~~ **Our** management has identified material weaknesses in our internal control over financial reporting and we may identify additional material weaknesses in the future or otherwise fail to maintain an effective system of internal controls, which may result in material misstatements of our financial statements or cause us to fail to meet our periodic reporting obligations, " we may need to undertake various **additional** costly and time-consuming actions, such as implementing new internal controls and procedures and hiring accounting or internal audit staff, which may adversely affect our business, financial condition and results of operations. We may not be able to complete our evaluation, testing and any required remediation in a timely manner. If we are unable to assert that our internal control over financial reporting is effective **and our independent registered public accounting firm is unable to attest to management' s assessment of the effectiveness of our internal control over financial reporting** , we could lose investor confidence in the

accuracy and completeness of our financial reports, which would cause the price of our common stock to decline, and we may be subject to investigation or sanctions by the SEC. We **are** ~~may be~~ required, pursuant to Section 404 of SOX, to furnish a report by management on, among other things, the effectiveness of our internal control over financial reporting as of December 31, ~~2022~~ **2023** ~~at the time we file our next Annual Report on Form 10- K~~ . This assessment will need to include disclosure of any material weaknesses identified by our management in our internal control over financial reporting, including the existing material weakness, if not remediated. We are also required to disclose changes made in our internal control and procedures on a quarterly basis **. In addition, our independent auditor is required to attest to management' s assessment of the effectiveness of our internal control over financial reporting** . Additionally, the existence of any material weakness, including our existing material weaknesses identified by management previously, or **any** significant deficiency requires management to devote significant time and incur significant expense to remediate any such material weaknesses or significant deficiencies and management may not be able to remediate any such material weaknesses or significant deficiencies in a timely manner. The existence of any material weakness in our internal control over financial reporting could also result in errors in our financial statements that could require us to restate our financial statements, cause us to fail to meet our reporting obligations and cause shareholders to lose confidence in our reported financial information, all of which could materially and adversely affect our business and stock price. Items 1B ~~, 2, 3,~~ and ~~4~~ **1C**