

Risk Factors Comparison 2024-02-29 to 2023-03-24 Form: 10-K

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

Our business involves significant risks and uncertainties, some of which are described below. You should carefully consider the risks and uncertainties described below, together with all of the other information in this Annual Report on Form 10-K. ~~The risks and uncertainties described below are not the only ones we face. Additional risk and uncertainties that we are unaware of or that we deem immaterial may also become important factors that adversely affect our business.~~ The realization of any of these risks and uncertainties could have a material adverse effect on our reputation, business, financial condition, results of operations, growth, and future prospects as well as our ability to accomplish our strategic objectives. In that event, the market price of our common stock could decline and you could lose part or all of your investment. Risks Related to Our Business We have a history of losses. We have not been profitable historically and may not achieve or maintain profitability in the future. We have a history of losses. Our ability to forecast our future operating results is subject to a number of uncertainties, including our ability to plan for and model future growth. We have encountered and will continue to encounter risks and uncertainties frequently experienced by growing companies in rapidly evolving industries. If our assumptions regarding these uncertainties, which we use to plan our business, are incorrect or change in reaction to changes in our markets, or if we do not address these risks successfully, our operating and financial results could differ materially from expectations, our business could suffer, and the trading price of our stock may decline. We have incurred net losses of \$ **106.3 million and \$** 86.4 million and \$ 10.9 million for the years ended December 31, **2023 and** 2022 and 2021, respectively. As of December 31, ~~2022~~ **2023**, we had an accumulated deficit of \$ **192.298.25** million. We are not certain whether or when we will obtain a high enough volume of sales of our products to sustain or increase our growth or achieve or maintain profitability in the future. We expect our costs to increase in future periods, which could negatively affect our future operating results if our revenue does not increase. In particular, we expect to continue to expend substantial financial and other resources on: • research and development related to our products, including investments in expanding our research and development team; • sales and marketing, including a significant expansion of our sales organization, both direct and through ~~channel-reseller~~ **channel-reseller** partners; • continued expansion of our business into new and adjacent vertical markets **and the launch of new product offerings**; and • general administration expenses, including legal and accounting expenses related to being a public company **and transitioning to large accelerated filer status**. These investments may not result in increased revenue or growth in our business. If we are unable to increase our revenue at a rate sufficient to offset the expected increase in our costs, our business, financial position, and results of operations will be harmed, and we may not be able to achieve or maintain profitability over the long term. Additionally, we may encounter unforeseen operating expenses, difficulties, complications, delays, and other unknown factors that may result in losses in future periods. If our revenue growth does not meet our expectations in future periods, our financial performance may be harmed, and we may not be able to achieve or maintain profitability in the future. Our operating results may fluctuate for a variety of reasons, including our failure to close large volume opportunity customer sales. A meaningful portion of our revenue is generated by product sales to new customers and sales of additional products to existing customers. The timing of certain large volume opportunities can impact ~~our~~ **the Company's** results from quarter to quarter. In addition, the sales cycle can last several months from initial engagement to contract negotiation and execution, culminating in delivery of our products to our customers, and this sales cycle can be even longer, less predictable and more resource-intensive for both larger volume sales as well as sales to customers in certain market segments. Customers may also require additional internal approvals or seek to pilot our products for a longer trial period before deciding to purchase our solutions. As a result, the timing of individual sales can be difficult to predict. In some cases, sales have occurred in a quarter subsequent to when anticipated, or have not occurred at all, which can significantly impact our quarterly financial results and make it more difficult to meet market expectations. See "Management's Discussion and Analysis of Financial Condition and Results of Operations — Critical Accounting Policies — Revenue Recognition." In addition to the sales cycle-related fluctuations noted above, our financial results, including our billings and deferred revenue, ~~will~~ **may** continue to vary **from period to period** as a result of numerous factors, many of which are outside of our control and may be difficult to predict, including: • our ability to attract and retain new customers; • our ability to sell additional Evolv Express systems to existing customers; • unforeseen changes or delays in our supply chain or third-party manufacturing partners; • our ability to expand into adjacent and complementary markets; • changes in customer or reseller partner requirements or market needs; • changes in the growth rate of the next-generation touchless security screening market; • the timing and success of new product introductions by us or our competitors, or any other change in the competitive landscape of the next-generation touchless security screening market, including consolidation among our customers or competitors or significant price competition; • a disruption in, or termination of, any of our relationships with reseller partners; • our ability to successfully expand our business globally; • reductions in customer retention rates, especially at subscription term expiration; • changes in our pricing policies or those of our competitors; • changes in financial markets or macroeconomic conditions, including, for example, due to the effects of ~~the ongoing recession~~ **recessionary or trends**, slow economic growth, **or political elections** in the United States and abroad, **rising inflation and high** interest rates, fuel prices, international currency fluctuations, corruption, political instability, **continuing social concerns and divisions in the United States and abroad**, acts of war, including the ~~conflict~~ **conflicts involving Russia in Europe and Ukraine the Middle East**, and acts of terrorism; • ~~general economic conditions in our markets, including recessionary pressures~~ **both domestic and international**; • future accounting pronouncements or changes in our accounting policies or practices; • the amount and timing of our operating costs, including cost of goods sold; • the impact of ~~any~~ **the COVID-19 pandemic, epidemic, and the emergence of new variants** or a future

outbreak of disease or similar public health concern, **such as COVID-19 (including the emergence of any new variants of COVID-19)** on our existing and new customers, partners, employees, and supply chain; and • increases or decreases in our revenue and expenses caused by fluctuations in foreign currency exchange rates. Any of the above factors, individually or in the aggregate, may result in significant fluctuations in our financial and other operating results from period to period. These fluctuations could result in our failure to meet our operating plan or the expectations of investors or analysts for any period. If we fail to meet such expectations for these or other reasons, the trading price of our common stock could fall substantially, and we could face costly lawsuits, including securities class action suits. We rely on reseller partners to generate a growing portion of our revenue, both in the United States and in emerging international markets which are generally slower to develop. If we fail to maintain successful relationships with our reseller partners, or if our partners fail to perform, our ability to market, sell and distribute our products will be limited, and our business, financial position and results of operations will be harmed. In addition to our direct sales force, we rely on our reseller partners to sell our products. We expect to continue to focus on generating sales to new and existing customers through our reseller partners as a part of our growth strategy. We provide our reseller partners with specific training and programs to assist them in selling and supporting our products, but there can be no assurance that these steps will be effective. In addition, our reseller partners may be unsuccessful in marketing, selling, and supporting our products. If we are unable to develop and maintain effective sales incentive programs for our third- party reseller partners, we may not be able to incentivize these partners to sell our products to customers and, in particular, to high profile public and private venues and institutions. Our agreements with our reseller partners are generally non- exclusive and these partners may also market, sell and support products that are competitive with us and may devote more resources to the marketing, sales and support of such competitive products. These partners may have incentives to promote our competitors' products to the detriment of ours or may cease selling our products altogether. Our reseller partners may cease or de- emphasize the marketing of our products with limited or no notice and with little or no penalty. Our agreements with our reseller partners may generally be terminated for any reason by either party with advance notice prior to each annual renewal date. It cannot be certain that we will retain these reseller partners or that we will be able to secure additional or replacement reseller partners. The loss of one or more of our significant reseller partners or a decline in the number or size of orders from them could harm our operating results. In addition, any new reseller partner requires extensive training and may take several months or more to achieve productivity. Our reseller partner sales structure could subject us to lawsuits, potential liability and reputational harm if, for example, any of our reseller partners misrepresent the functionality of our products, subscriptions or services to customers, or violate laws or our corporate policies. If we fail to effectively manage our existing resellers, or if our reseller partners are unsuccessful in fulfilling the orders for our products, or if we are unable to enter into arrangements with, and retain a sufficient number of, high quality reseller partners in each of the regions in which it sells products and keep them motivated to sell our products, our ability to sell our products and operating results will be harmed. The termination of our relationship with any significant reseller partner may also adversely impact our sales and operating results. We may not be successful in our **distributor licensing agreement with our third- party manufacturer. As part of our overall** strategy to move away from purchase subscription contracts **in favor of pure subscription contracts, which could have an adverse impact on our business, financial position and results of operations.** We are transitioning our go- to- market strategy to focus on our "pure subscription" sales model, where the customer leases our hardware, as opposed to purchasing the hardware outright, and enters into a multi- year security- as- a- service subscription. The pure subscription model aligns more closely with the SaaS nature of our business and results in a more predictable and consistent recurring revenue stream as compared to the purchase subscription model. This strategy depends in part on our ability to drive increased pure subscription contracts through our reseller partners. During 2022, the majority of our sales, and the vast majority of sales made through our reseller partners, were in the form of purchase subscription contracts. We and / or our resellers may not be as successful at marketing pure subscription contracts to prospective end- use customers, which would negatively impact our sales growth. As part of this overall strategy, we entered into a distributor licensing agreement with Columbia Tech in March 2023. Under this arrangement, we have granted a license of our intellectual property to Columbia Tech, who **will contract contracts** directly with certain of our resellers to fulfill the sales demand where the end- user customer requires the contract to be in form of a hardware purchase, instead of leasing our hardware. Columbia Tech **will pay pays** us a hardware license fee for each **Evolv Express** system **sold- it manufactures and sells** under this agreement. In these instances, we **will** still contract directly with the reseller to provide a multi- year security- as- a- service subscription to the end- users. Columbia Tech is an independent entity subject to its own unique operational and financial risks which are out of our control. Further, Columbia Tech does not regularly act in the capacity of a distributor for the products it manufactures. If Columbia Tech fails to perform as required under the distributor licensing agreement, this could impair the reputation of our company and our products, our relationships with resellers, our ability to earn revenue from SaaS subscription contracts, and our ability to receive license fees from **it under the distributor licensing agreement, any of which could, in turn, adversely impact** our **contract manufacturer- business, financial position, and results of operations**. Increases in component costs, long lead times, supply shortages, and supply changes could disrupt our supply chain and have an adverse effect on our business, financial condition, and operating results. We acquire certain of our materials, which are critical to the ongoing operation and future growth of our business, from several third parties, both foreign and domestic. Generally, our third- party contract manufacturers contract directly with component suppliers, and we rely on our contract manufacturers to manage their supply chains. **Our if our contract manufacturers have experienced, and may in the future experience any, supply chain disruptions as a result of COVID- 19 or other similar health crises as well as global economic impacts or other changes in macroeconomic trends. In the event our contract manufacturers are unable to adequately manage their supply chain** or our relationships with our contract manufacturers terminate, we could experience delays, which could negatively impact our business, customer relationships, and margins. We also source some materials and components directly from suppliers. While most components and materials for our products are available from multiple suppliers, certain of those items are only available from limited or sole sources. Should any

of these suppliers become unavailable or inadequate, or impose terms unacceptable to us, such as increased pricing terms, we could be required to spend a significant amount of time and expense to develop alternate sources of supply, and may not be successful in doing so on terms acceptable to it, or at all. As a result, the loss of a limited or sole source supplier could adversely affect our manufacturing capacity, and relationships with our customers, as well as our results of operations and financial condition. We depend on **our primary** third-party contract manufacturer for the production of our touchless security screening systems. While there are several potential **contract** manufacturers for most of these products, all our **products-systems** are currently manufactured, assembled, tested **and**, **and** packaged by **Columbia Tech** a third-party manufacturer located in Massachusetts. In most cases, we rely on this manufacturer to procure components and, in some cases, provide manufacturing engineering work. Although we are seeking to expand and diversify our contract manufacturer relationships, our current reliance on one contract **manufacturing manufacturer** involves several risks, including: • unexpected increases in manufacturing and repair costs; • inability to control the quality and reliability of finished **products-systems**; • inability to control delivery schedules; • potential liability for expenses incurred by the third-party contract manufacturer in reliance on our forecasts that later prove to be inaccurate; • potential lack of adequate capacity to manufacture all **of components or part parts** of the products we require; • **potential labor unrest or unavailability affecting the ability of the third-party manufacturers to produce our systems; and** • the occurrence of unforeseen force majeure events **; and** • **potential labor unrest or unavailability affecting the ability of the third-party manufacturers-- manufacturer to produce our products**. We also use a third-party contract manufacturer located in Massachusetts as a second source for the production of a key sensor component used in our touchless security screening systems. If our third-party contract manufacturers experience a delay, disruption, or quality control problems in its operations or if the third-party contract manufacturers do not renew or terminate our agreement with them, our operations could be significantly disrupted and our product shipments could be delayed. Qualifying new manufacturers and commencing volume production is expensive and time consuming. Ensuring that a contract manufacturer is qualified to manufacture our products or components to our standards is time consuming. In addition, there is no assurance that contract manufacturers can scale their production of our products or components at the volumes and in the quality that we require. If contract manufacturers are unable to do these things, we may have to move production for the products or components to a new or existing third-party manufacturer, which would take significant effort and our business, results of operations and financial condition could be materially adversely affected. As we contemplate moving manufacturing into different jurisdictions, we may be subject to additional and significant challenges in ensuring that quality, processes, and costs, among other issues, are consistent with our expectations. For example, while we expect our third-party contract manufacturers to be responsible for penalties assessed on us because of excessive failures of the products or warranty claims, there is no assurance that we will be able to collect such reimbursements from these manufacturers, which causes **it-us** to take on additional risk for potential failures of our products. In addition, because we currently use third-party contract manufacturers to produce our touchless security screening systems and certain key components, increases in the prices charged may have an adverse effect on our results of operations, as we may be unable to find **a contract manufacturer manufacturers** who can supply us at a lower price. As a result, the loss of a limited or sole source supplier could adversely affect our relationships with our customers and our results of operations and financial condition. Our **business operations** **third-party contract manufacturers' facilities, and our suppliers' and our customers' facilities,** are vulnerable to disruption due to natural or other disasters, including climate-related events, strikes, and other events beyond our control. A major earthquake, fire, tsunami, hurricane, cyclone, or other disaster, such as a major flood, seasonal storms, drought, extreme temperatures, nuclear event, or terrorist attack affecting our facilities or the areas in which we are located, or affecting those of our customers or third-party manufacturers or suppliers, could significantly disrupt our or their operations and delay or prevent product shipment or installation during the time required to repair, reinforce, rebuild or replace our or their damaged manufacturing facilities. These delays could be lengthy and costly. Climate change may contribute to increased frequency or intensity of certain of these events, **including increasing frequency and severity of storms, floods, drought, water scarcity, heat waves, wildfires and resultant air quality impacts and power shutoffs associated with these types of events, or a significant power outage** as well as contribute to chronic changes in the physical environment (such as changes to ambient temperature and precipitation patterns or sea-level rise) that may impair the operating conditions of these facilities, or otherwise adversely impact our operations. If our third-party contract manufacturers', suppliers', or customers' facilities are negatively impacted by such a disaster, production, shipment, and installation of our products could be delayed, which can impact the period in which it recognizes the revenue related to that product sale. Additionally, customers may delay purchases of our products until operations return to normal. Even if we can respond quickly to a disaster, the continued effects of the disaster could create uncertainty in our business operations. **Climate-related events, including the increasing frequency of extreme weather events and their impact on critical infrastructure in the United States and elsewhere, have the potential to disrupt businesses in general and may cause us to experience higher attrition, losses, and additional costs to maintain and resume operations. Transitional climate change risks that result from a shift to a low-carbon economy may also subject us to increased regulations, reporting requirements, standards, or expectations regarding the environmental impacts of our business and untimely or inaccurate disclosure could adversely affect our reputation, business, or financial performance.** In addition, concerns about terrorism, the effects of a terrorist attack, political turmoil, **strikes or other labor strikes unrest**, war, including **Russia's invasion of Ukraine in Europe and the Middle East**, and the related geopolitical impacts, or the outbreak of epidemic diseases (including such as the on-going COVID-19 pandemic) could have a negative effect on **our-the** operations **of our facilities and those of our contract manufacturers, suppliers and customers, resulting in delays or other challenges in the deployment of our products and services, among others, and thereby negatively impact our** sales. We recognize a substantial portion of our revenue ratably over the term of our agreements with customers and, as a result, downturns or upturns in sales may not be immediately reflected in our operating results. We recognize a substantial portion of our revenue ratably over the terms of our agreements with customers, which generally occurs

over a four- year period. As a result, a substantial portion of the revenue that we report in each period will be derived from the recognition of deferred revenue relating to agreements entered into during previous periods. Consequently, a decline in new sales or renewals in any one period may not be immediately reflected in our revenue results for that period. This decline, however, will negatively affect our revenue in future periods. Accordingly, the effect of significant downturns in sales and market acceptance of our products, and potential changes in our rate of renewals may not be fully reflected in our results of operations until future periods. Our model also makes it difficult to rapidly increase our revenue through additional sales in any period, as revenue from new customers generally will be recognized over the term of the applicable agreement. We also intend to increase our investment in research and development, sales and marketing, and general and administrative functions and other areas to grow our business. These costs are generally expensed as incurred (with the exception of sales commissions), as compared to our revenue, a substantial portion of which is recognized ratably in future periods. We are likely to recognize the costs associated with these increased investments earlier than some of the anticipated benefits and the return on these investments may be lower, or may develop more slowly, than ~~it we expects~~ **expect**, which could adversely affect our operating results. The AI- based weapons detection for security screening market is new and evolving and may not grow as expected or may develop more slowly or differently than we expect. If the market does not grow as we expect, or if we cannot expand our solutions to meet the demands of this market, our revenue may decline, fail to grow or fail to grow at an accelerated rate, and we may incur operating losses. We believe our future success will depend in large part on the growth, if any, in the market for AI- based weapons detection for security screening solutions. This market is new and evolving, and as such, it is difficult to predict important market trends, including our potential growth, if any. To date, enterprise and corporate security budgets have allocated a majority of dollars to conventional security solutions, such as lower priced walk- through metal detectors. Organizations that use these security products may be satisfied with them or slow to adapt to technical advances and, as a result, these organizations may not adopt our solutions in addition to, or in lieu of, security products they currently use. Further, sophisticated attackers are skilled at adapting to new technologies and developing new methods of breaching organizations' security systems, and changes in the nature of security threats could result in a shift in budgets away from products such as ours. In addition, while recent high visibility attacks at publicly and privately- owned venues and schools have increased market awareness of mass shootings, terrorist, or other attacks, if such attacks were to decline, or enterprises or governments perceived that the general level of attacks has declined, our ability to attract new customers and expand our sales to existing customers could be materially and adversely affected. If products such as ours are not viewed by organizations as necessary, or if customers do not recognize the benefit of our products as a critical element of an effective security strategy, our revenue may not grow as quickly as expected, or may decline, and the trading price of our stock could suffer. In addition, it is difficult to predict customer adoption and retention rates, customer demand for our products, the size and growth rate of the market for AI- based weapons detection for security screening, the entry of competitive products, or the success of existing competitive products. Any expansion in our market depends on a number of factors, including the cost, performance, and perceived value associated with our products and those of our competitors. If these products do not achieve widespread adoption or there is a reduction in demand for products in our market caused by a lack of customer acceptance, technological challenges, regulatory restrictions, competing technologies or products, decreases in corporate spending, weakening economic conditions or otherwise, it could result in reduced customer orders, early terminations, reduced customer retention rates or decreased revenue, any of which would adversely affect our business operations and financial results. You should consider our business and prospects in light of the risks and difficulties it may encounter in this new and evolving market. **We use machine learning, artificial intelligence, and automated decision making in our development process and in our AI- based weapon detection products. Machine learning, artificial intelligence and automated decision making technologies may not be accurate and we may not be able to protect our intellectual property rights related to products or services created with machine learning, artificial intelligence and automated decision making. We use machine learning, artificial intelligence, and automated decision making technologies, including propriety artificial intelligence and machine learning algorithms, in the development and operation of our AI- based weapons detection products for security screening. There are significant risks involved in developing, maintaining, and deploying machine learning and artificial intelligence technologies and there can be no assurance that the usage of such technologies will always enhance our products or services or be beneficial to our business, including our efficiency or profitability. In particular, if these artificial intelligence or machine learning models are incorrectly designed or implemented; trained or reliant on incomplete, inadequate, inaccurate, biased or otherwise poor quality data or on data to which we do have sufficient rights; and / or are adversely impacted by unforeseen defects, technical challenges, cyber security threats or material performance issues, the performance of our products, services, and business, as well as our reputation and the reputations of our customers, could suffer or we could incur liability through the violation of laws or contracts to which we are a party or civil claims. Further, our ability to continue to develop or use such technologies may be dependent on access to specific third- party software and infrastructure, such as processing hardware or third- party artificial intelligence models, and we cannot control the availability or pricing of such third party software and infrastructure, especially in a highly competitive environment. In addition, market acceptance and consumer perceptions of artificial intelligence and machine learning technologies are uncertain. A number of aspects of intellectual property protection in the field of artificial intelligence and machine learning are currently under development, and there is uncertainty and ongoing litigation in different jurisdictions as to the degree and extent of protection warranted for artificial intelligence and machine learning systems and relevant system input and outputs. If we fail to obtain protection for the intellectual property rights concerning our artificial intelligence and machine learning technologies, or later have our intellectual property rights invalidated or otherwise diminished, our competitors may be able to take advantage of our research and development efforts to develop competing products.** If we are unable to acquire new customers, our future revenues and operating results will be harmed.

Likewise, potential customer turnover in the future, or costs we incur to retain our existing customers, could materially and adversely affect our financial performance. Our success depends on our ability to acquire new customers in new and existing vertical markets, and in new and existing geographic markets. If we are unable to attract a sufficient number of new **customers and retain our existing** customers, we may be unable to generate revenue growth at desired rates. The physical security solutions market is competitive, and many of our competitors have **substantial, significantly greater** financial, personnel, and other resources ~~that than they utilize~~ **we do and may be able to devote greater resources to their efforts** to develop solutions and attract customers. As a result, it may be difficult for us to add new customers to our customer base. Competition in the marketplace may also lead us to win fewer new customers or result in us providing discounts and other commercial incentives **to win new customers or retain our existing customers**. Additional factors that impact our ability to acquire new **customers and retain existing** customers include the perceived need for AI- based weapons detection for security solutions, the size of our prospective customers' security budgets, the availability of government funding, the utility and efficacy of our existing and new products **or product enhancements**, whether proven or perceived, and general economic conditions. These factors may have a meaningful negative impact on **our** future revenues and operating results. While our immediate focus is on the United States market, our long- term success in part depends on our ability to acquire new customers outside the United States. The United States has significantly more privately owned firearms than any other country. If customers in other countries do not perceive the threat of firearms and weapons to be significant enough to justify the purchase of our products, we will be unable to establish a meaningful business outside the United States. If we are unable to attract a sufficient number of new customers outside the United States, we may be unable to generate future revenue growth at desired rates in the long term. If we are unable to sell additional ~~existing and new~~ products to our customers and maintain and grow our customer retention rates, our future revenue and operating results will be harmed. Our future success depends, in part, on our ability to expand the deployment of our products with existing customers by selling them additional Evolv Express systems. This may require increasingly sophisticated and costly sales efforts and may not result in additional sales. In addition, the rate at which our customers purchase additional products depends on a number of factors, including the perceived need for additional touchless security screening solutions as well as general economic conditions. If our efforts to sell additional products to our customers are not successful, our business may suffer. If our products fail or are perceived to fail to detect threats such as a firearm or other potential weapon or explosive device, or if our products contain undetected errors or defects, these failures or errors could result in injury or loss of life, which could harm our brand and reputation and have an adverse effect on our business and results of operations. If our products fail or are perceived to fail to detect and prevent attacks or if our products fail to identify and respond to new and increasingly complex and unpredictable methods of attacks, our business and reputation may suffer. There is no guarantee that our products will detect and prevent all attacks, especially in light of the rapidly changing security landscape to which it must respond, as well as unique factors that may be present in our customers' operating environments. Additionally, our products may falsely detect items that do not actually represent threats. These false positives may impair the perceived reliability of our products, and may therefore adversely impact market acceptance of our products, ~~and~~ **which could, in turn,** result in negative publicity, loss of customers and sales, and increased costs to remedy any problem. Our products, which are complex, may also contain undetected errors or defects when first introduced or as new versions are released. We have experienced these errors or defects in the past in connection with new products and product upgrades. We expect that these errors or defects will be found from time to time in the future in new or enhanced products after commercial release. Defects may result in increased vulnerability to attacks, cause our products to fail to detect security threats, or temporarily interrupt our products' ability to screen visitors in a customer' s location. Any errors, defects, disruptions in service or other performance problems with our products may damage our customers' business and could harm our reputation. If our products fail to detect security threats for any reason, including failures due to customer personnel or security processes, it may result in significant costs, the attention of our key personnel could be diverted, our customers may delay or withhold payment to us or elect not to renew or cause other significant customer relations problems to arise. We may also be subject to liability claims for damages related to errors or defects in our products. For example, if our products fail to detect weapons or explosive devices that are subsequently used by terrorists, criminals, or unbalanced individuals to cause casualties at a high profile, public venue, we could incur financial damages and our reputation could also be significantly harmed. A material liability claim or other occurrence that harms our reputation or decreases market acceptance of our products may harm our business and operating results. Although we have limitation of liability provisions in our terms and conditions of sale, they may not fully or effectively protect us from claims as a result of federal, state, or local laws or ordinances, or unfavorable judicial decisions in the United States or other countries. The sale and support of our products also entails the risk of product liability claims. We maintain insurance to protect against certain claims associated with the use of our products, but our insurance coverage may not adequately cover any claim asserted against us. In addition, even claims that ultimately are unsuccessful could result in our expenditure of funds in litigation, divert or distract management' s time and other resources, and harm our business and reputation. The loss of designation of our Evolv Express system as a Qualified Anti- Terrorism Technology under the Homeland Security SAFETY Act could result in adverse reputational and financial consequences. Our Evolv Express system has been awarded the ~~U. S. Department of Homeland Security ("DHS ")~~ SAFETY Act Designation as a Qualified Anti- Terrorism Technology. Technologies that are awarded the SAFETY Act Designation have undergone rigorous use and review to meet and / or exceed the DHS' performance standards that include examination of test results for weapons detection, operational use and effectiveness, manufacturing and quality assurance practices, and customer feedback. Any amendments or interpretive guidance related to the SAFETY Act may affect our ability to retain our SAFETY Act Designation, may increase the costs of compliance, and / or may negatively impact our ability to attract new customers. Because we view our SAFETY Act Designation as a differentiating factor among our industry peers, if laws and regulations change relating to the SAFETY Act or if we fail to comply with the SAFETY Act' s requirements, our business, financial condition, results of operations, and stock price could be materially and adversely affected. If we do not

successfully anticipate market needs and enhance our existing products or develop new products that meet those needs on a timely basis, we may not be able to compete effectively and our ability to generate revenues will suffer. Our customers face evolving security risks that require them to adapt to increasingly complex infrastructures that incorporate a variety of security solutions. We face significant challenges in ensuring that our products effectively identify and respond to these security risks without disrupting the performance of our customers' infrastructures. As a result, we must continually modify and improve our products in response to changes in our customers' infrastructures. We cannot guarantee that we will be able to anticipate future market needs and opportunities or be able to develop product enhancements or new products to meet such needs or opportunities in a timely manner, if at all. Even if we are able to anticipate, develop and commercially introduce enhancements and new products, there can be no assurance that enhancements or new products will achieve widespread market acceptance. New products, as well as enhancements to our existing products, could fail to attain sufficient market acceptance for many reasons, including: • delays in releasing new products or product enhancements; • failure to accurately predict market demand and to supply products that meet this demand in a timely fashion; • inability to protect against new types of attacks or techniques used by terrorists or other threat sources; • defects in our products, errors or failures of our products; • negative publicity or perceptions about the performance or effectiveness of our products; • introduction or anticipated introduction of competing products by our competitors; • installation, configuration, sensitivity setting, or usage errors by our customers; and • easing or changing of regulatory requirements at the federal, state, and / or local levels related to security or other aspects of our business. If we fail to anticipate market requirements or fail to develop and introduce product enhancements or new products to meet those needs in a timely manner, it could cause us to lose existing customers and prevent us from gaining new customers, which would significantly harm our business, financial condition, and results of operations. While we continue to invest significant resources in research and development to enable our products to continue to address the security risks that our customers face, the introduction of products embodying new technologies could also render our existing products or services obsolete or less attractive to customers. If we spend significant time and effort on research and development and are unable to generate an adequate return on our investment, our business and results of operations may be materially and adversely affected. Our business model is predicated, in part, on building a customer base that will generate a recurring stream of revenues through the sale of our subscription contracts. If that recurring stream of revenues does not develop as expected, or if our business model changes as the industry evolves, our operating results may be adversely affected. Our business model is dependent, in part, on our ability to maintain and increase subscriptions for our proprietary products as they generate recurring revenues. Existing and future customers of our products may not purchase our subscriptions for our proprietary products at the same rate at which customers currently purchase those subscriptions. If our current and future customers purchase a lower volume of our subscriptions for our proprietary products, our recurring revenue stream relative to our total revenues would be reduced and our operating results would be adversely affected. A portion of our revenue is generated by sales to government entities and such sales are subject to a number of challenges and risks. Approximately 4% and 1% of our revenue was generated by sales to government entities during each of the years ended December 31, 2022-2023 and December 31, 2021-2022, respectively. Selling to government entities can be highly competitive, expensive, and time-consuming, and often requires significant upfront time investment and expense without any assurance of winning that it will win a sale sales contract. Government demand and payment for our solutions may also be impacted by changes in fiscal or contracting policies, changes in government programs or applicable requirements, the adoption of new laws or regulations or changes to existing laws or regulations, public sector budgetary cycles and funding authorizations, with funding reductions or delays adversely affecting public sector demand for our solutions. Accordingly, increasing sales of our products to government entities may be more challenging than selling to commercial organizations, especially given extensive certification, compliance, clearance, and security requirements. Government agencies may have statutory, contractual, or other legal rights to terminate contracts with us or reseller partners. Further, in the course of providing our solutions to government entities, our employees and those of our reseller partners may be exposed to sensitive government information. Any failure by us or our reseller partners to safeguard and maintain the confidentiality of such information could subject us to liability and reputational harm, which could materially and adversely affect our results of operations and financial performance. Governments routinely investigate and audit government contractors' administrative processes, and any unfavorable audit may cause the government to shift away from our solutions and may result in a reduction of revenue, fines or civil or criminal liability if the audit uncovers improper or illegal activities, which could adversely impact our results or operations. Downturns in general economic and market conditions and reductions in spending may reduce demand for our products and services and may impact third parties on which we rely, which could harm our revenue, results of operations, and cash flows, and could make it difficult to predict revenue for a particular period. Our revenue depends significantly on general economic conditions and the level of concern regarding physical security and, which impacts the public's willingness to attend live events or otherwise gather in numbers. Economic weakness, customer financial difficulties and constrained spending on security measures may result in decreased revenue and earnings. Further worsening, broadening or protracted extension of an economic downturn could have a material negative impact on our business, revenue, results of operations, and cash flows. In addition, concerns regarding continued budgetary challenges in the United States and Europe, increasing high interest rates in the United States and around the world, an a sustained-inflationary environment, recessionary pressures, geopolitical turmoil (including Russia's invasion of Ukraine in Europe and the Middle East) and terrorism in many parts of the world, and the effects of climate change have and may continue to put pressure on global economic conditions and level of concern regarding physical security concerns. If we do not succeed in convincing customers that our products should be an integral part of their overall approach to security and that a fixed portion of their annual security budgets should be allocated to our products, general reductions in security spending by our customers are likely to have a disproportionate impact on our business, results of operations, and financial condition. General economic weakness may also lead to longer collection cycles for payments due from our customers, an increase in customer bad debt, restructuring initiatives and associated expenses

and impairment of investments. Furthermore, the continued weakness and uncertainty in worldwide credit markets, including the sovereign debt situation in certain countries in the European Union, or ("the" EU,") may adversely impact the ability of our customers to adequately fund their expected capital expenditures, which could lead to delays or cancellations of planned purchases of our products. We also face risks from financial difficulties or other uncertainties experienced by our suppliers, channel reseller partners, or other third parties on which we rely. If our partners and suppliers are negatively impacted by declining economic conditions or circumstances arising from military conflicts, and such third parties are unable to supply us with required materials or components or otherwise assist us in operating our business, our business could be harmed. In addition, military conflicts, such as Russia's invasion of Ukraine including those in Europe and the Middle East, have and could continue to disrupt or otherwise adversely impact our operations and those of third parties upon which we rely. Related sanctions, export controls, and other actions have and may in the future be initiated by nations including the United States, the EU, China, or Russia (such as potential cyberattacks, disruption of energy flows, and others), which could adversely affect our business and / or our supply chain. Uncertainty about future economic conditions and market volatility also makes it difficult to forecast operating results and to make decisions about future investments. Future or continued economic weakness for us or our customers, failure of our customers and markets to recover from such weakness, customer financial difficulties, and reductions in spending on security systems could have a material adverse effect on demand for our products, and consequently on our business, financial condition, and results of operations. Our brand, reputation, and ability to attract, retain, and serve our customers are dependent in part upon the reliable performance of our products, infrastructure, and employees. Our brand, reputation, and ability to attract, retain, and serve our customers are dependent in part upon the reliable performance of, and the ability of our existing customers and new customers to access and use, our solutions, including real-time analytics and intelligence. We have experienced, and may in the future experience, disruptions, outages, and other performance problems due to a variety of factors, including infrastructure changes, equipment failure, human or software errors, capacity constraints, and fraud or cybersecurity attacks. In some instances, we may not be able to identify the cause or causes of these performance problems within an acceptable period of time. Interruptions in our systems or the third-party systems on which we rely, whether due to system failures, computer viruses, physical or electronic break-ins, or other factors, could affect the security or availability of our products, network infrastructure, cloud infrastructure, and website. Problems with the reliability or security of our systems could harm our reputation. Damage to our reputation and the cost of remedying these problems could negatively affect our business, financial condition, and operating results. Additionally, our third-party hosting suppliers have no obligations to renew their agreements with us on commercially reasonable terms or at all, and certain of the agreements governing these relationships may be terminated by either party at any time. If we are unable to maintain, renew, or expand our agreements with these providers on commercially reasonable terms, we may experience costs or downtime as we transition our operations. Any disruptions or other performance problems with our products could harm our reputation and business and may damage our customers' businesses. Interruptions in our service delivery might reduce our revenue, cause us to issue credits to customers, subject us to potential liability, and cause customers not to renew their subscription purchases of our products. If we do not effectively expand, train, and retain qualified sales and marketing personnel, we may be unable to acquire new customers or sell additional products to successfully pursue our growth strategy. We depend significantly on our sales force to attract new customers and expand sales to existing customers. As a result, our ability to grow our revenue depends in part on our success in recruiting, training, and retaining sufficient numbers of sales personnel to support our growth, particularly in the United States and, to a more limited extent, internationally. The number of our sales and marketing personnel increased from 91-97 as of December 31, 2021-2022 to 97-139 as of December 31, 2022-2023. We expect to continue to expand our sales and marketing personnel and face a number of challenges in achieving our hiring and integration goals. There is intense competition for individuals with sales training and experience. In addition, the training and integration of a large number of sales and marketing personnel in a short time requires the allocation of significant internal resources. We invest significant time and resources in training new sales force personnel to understand our products, platform, and our growth strategy. Based on our past experience, it takes approximately six to 12 months before a new sales force member operates at target performance levels, depending on their role. However, we may be unable to achieve or maintain our target performance levels with large numbers of new sales personnel as quickly as we have done in the past. Our failure to hire a sufficient number of qualified sales force members and train them to operate at target performance levels may materially and adversely impact our projected growth rate. If we are not able to maintain and enhance our brand or reputation as an industry leader, our business and operating results may be adversely affected. We believe that maintaining and enhancing our reputation as the leader in next-generation AI-based weapons detection for security screening is critical to our relationship with our existing end-user customers and reseller partners and our ability to attract new customers and reseller partners. The successful promotion of our brand will depend on multiple factors, including our marketing efforts, our ability to continue to deliver a superior customer experience and develop high-quality features for our products, and our ability to successfully differentiate our products from those of our competitors. Our brand promotion activities may not be successful or yield increased revenue. Additionally, the performance of our reseller partners may affect our brand and reputation if customers do not have a positive experience with our products as implemented by our reseller partners or with the implementation generally. The promotion of our brand requires us to make substantial expenditures, and we anticipate that the expenditures will increase as our market becomes more competitive, as we expand into new geographies and vertical markets and as more sales are generated through our reseller partners. To the extent that these activities yield increased revenue, this such increase in revenue may not offset the corresponding increased increase in expenses we incur. If we do not successfully maintain and enhance our brand and reputation, our business and operating results may be adversely affected. If our customers are unable to implement our products successfully, or if we fail to effectively assist our customers in installing our products and provide effective ongoing support and training, customer perceptions of our products may be impaired, or our reputation and brand may suffer. Our products are deployed in a wide variety of indoor and outdoor

environments, including large venues with multiple entry points. Some of our customers have experienced difficulties implementing our products in the past and may experience implementation difficulties in the future. If our customers are unable to implement our products successfully, customer perceptions of our products may be impaired, or our reputation and brand may suffer. Any failure by our customers to appropriately implement our products or any failure of our products to effectively integrate and operate within our customers' operating environments could result in customer dissatisfaction, impact the perceived reliability of our products, result in negative press coverage, negatively affect our reputation, and harm our financial results. Successful deployment and operation of our products depend on the knowledge and skill of the customer security personnel or implementation contractors charged with setting up, configuring, monitoring, and troubleshooting the equipment in their own environment. Many of our customers experience relatively high turnover in their security personnel, creating opportunities for knowledge and skill gaps that can result, and have resulted, in configuration, sensitivity setting, or operational errors that allow prohibited threats into customer facilities. In these situations, customers can perceive, and have perceived, that our products have failed to perform as designed until and unless we have been able to demonstrate otherwise. There can be no assurance that we or our implementation partners will successfully isolate and identify failures due to customer error in the future, and this could result in customer dissatisfaction, impact the perceived reliability of our products, result in negative press coverage, negatively affect our reputation, and harm our financial results. Our customers depend in large part on customer support delivered by us to resolve issues relating to the use of our products. However, even with our support, our customers are ultimately responsible for effectively using our products and ensuring that their staff is properly trained in the use of our products. The failure of our customers to correctly use our products, or our failure to effectively assist customers in installing our products and provide effective ongoing support and training, may result in an increase in the vulnerability of our customers' facilities and visitors to security threats. We are also in the process of expanding our customer success and support organizations, including the engagement and training of third-party contractors. It can take significant time and resources to recruit, hire and train qualified technical support and service employees and contractors. We may not be able to keep up with demand, particularly if the sales of our products exceed our internal forecasts. To the extent that we are unsuccessful in hiring, training, and retaining adequate support resources, our ability to provide adequate and timely support to our customers may be negatively impacted, and our customers' satisfaction with our products may be adversely affected. Additionally, in unusual circumstances, if ~~we it were to need needed~~ to rely on our sales engineers to provide post-sales support while ~~we are~~ growing our service organization, our sales productivity may be negatively impacted. Accordingly, any failure by us to provide satisfactory maintenance and technical support services could have a material and adverse effect on our business and results of operations. We are dependent on the continued services and performance of our senior management and other key employees, as well as on our ability to successfully hire, train, manage, and retain qualified personnel, especially those in sales and marketing and research and development. Our future performance depends on the continued services and contributions of our senior management, particularly Peter George, our President and Chief Executive Officer, and other key employees to execute on our business plan and to identify and pursue new opportunities and product innovations. We do not maintain key man insurance for any of our executive officers or key employees. From time to time, there may be changes in our senior management team resulting from the termination or departure of our executive officers and key employees. Our senior management and key employees are generally employed on an at-will basis, which means that they could terminate their employment with us at any time. The loss of the services of our senior management, particularly Mr. George and our founders, or other key employees for any reason could significantly delay or prevent our development or the achievement of our strategic objectives and harm our business, financial condition, and results of operations. Our ability to successfully pursue our growth strategy will also depend on our ability to attract, motivate, and retain our personnel, especially those in sales and marketing and research and development. We face escalating compensation demands from new and prospective employees, as well as intense competition for these employees from numerous technology, software, and other companies, especially in certain geographic areas in which we operate, and we cannot ensure that we will be able to attract, motivate and / or retain additional qualified employees in the future. If we are unable to attract new employees and retain our current employees, we may not be able to adequately develop and maintain new products, or market our existing products at the same levels as our competitors ~~and it may, therefore, which~~ **may lead us to** lose customers and market share. ~~our~~ **Our** failure to attract and retain personnel, especially those in sales and marketing, research and development, and engineering positions, could have an adverse effect on our ability to execute our business objectives ~~and, as a result, our ability to compete could decrease, our operating results could suffer and our revenue could decrease.~~ **Any of these factors may adversely impact our ability to compete and cause our revenue to decrease and our operating results to suffer.** We incorporate technology and components from third parties into our products, and our inability to obtain or maintain rights to the technology could harm our business. We incorporate technology and components from third parties into our products. We cannot be certain that our suppliers and licensors are not infringing the intellectual property rights of third parties or that the suppliers and licensors have sufficient rights to the technology in all jurisdictions in which it may sell our products. We may not be able to rely on indemnification obligations of third parties if some of our agreements with our suppliers and licensors may be terminated for convenience by them. If we are unable to obtain or maintain rights to any of this technology because of intellectual property infringement claims brought by third parties against our suppliers and licensors or against us, or if we are unable to continue to obtain such technology or enter into new agreements on commercially reasonable terms, our ability to develop and sell products, subscriptions, and services containing such technology could be severely limited, and our business could be harmed. Disputes with suppliers and licensors over uses or terms could result in the payment of additional royalties or penalties by us, cancellation or non-renewal of the underlying license or litigation. In the event that we cannot renew and / or expand existing licenses, we may be required to discontinue or limit our use of the operations, products, or

offerings that include or incorporate the licensed intellectual property. Any such discontinuation or limitation could have a material and adverse impact on our business, financial condition, and results of operation. Additionally, if we are unable to obtain necessary technology and components from third parties, including certain sole suppliers, we may be forced to acquire or develop alternative technology or components, which may require significant time, cost, and effort and may be of lower quality or performance standards. This would limit or delay our ability to offer new or competitive products and increase our costs of production. If alternative technology or components cannot be obtained or developed, we may not be able to offer certain functionality as part of our products, subscriptions, and services. As a result, our margins, market share and results of operations could be significantly harmed. Our use of “ open source ” software could subject our proprietary software to general release, negatively affect our ability to offer our products and subject us to possible litigation. We have used “ open source ” software in connection with the development and deployment of our software products, and we expect to continue to use open source software in the future. Open source software is licensed by its authors or other third parties under open source licenses, which in some instances may subject us to certain unfavorable conditions, including requirements that we offer our products that incorporate the open source software for no cost, that we make publicly available all or part of the source code for any modifications or derivative works we create based upon, incorporating or using the open source software, or that we license such modifications or derivative works under the terms of the particular open source license. Companies that incorporate open source software into their products have, from time to time, faced claims challenging the use of open source software and compliance with open source license terms. As a result, we could be subject to suits by parties claiming ownership of what we believe to be open source software or claiming noncompliance with open source licensing terms. While we monitor our use of open source software and try to ensure that none is used in a manner that would require us to disclose our proprietary source code or that would otherwise breach the terms of an open source agreement, we cannot guarantee that we will be successful, that all open source software is reviewed prior to use in our products, that our developers have not incorporated open source software into our products that we are unaware of or that they will not do so in the future. Furthermore, there are an increasing number of open source software license types, almost none of which have been interpreted by U. S. or foreign courts, resulting in a dearth of guidance regarding the proper legal interpretation of such licenses. As a result, there is a risk that open source software licenses could be construed in a manner that imposes unanticipated conditions or restrictions on our ability to market or provide our products and services. If we are held to have breached or failed to fully comply with all the terms and conditions of an open source software license, we could face infringement claims or other liability, or be required to seek costly licenses from third parties to continue providing our offerings on terms that are not economically feasible, if at all, to re- engineer all or a portion of our products, to discontinue or delay the provision of our offerings if re- engineering could not be accomplished on a timely basis or to make generally available, in source code form, our proprietary code. Further, in addition to risks related to license requirements, use of certain open source software carries greater technical and legal risks than does the use of third- party commercial software. For example, open source software is generally provided without any support or warranties or other contractual protections regarding infringement or the quality of the code, including the existence of security vulnerabilities. To the extent that our products ~~depends~~ **depend** upon the successful operation of open source software, any undetected errors or defects in open source software that we use could prevent the deployment or impair the functionality of our systems and injure our reputation. In addition, the public availability of such software may make it easier for others to compromise our products. Any of the foregoing risks could materially and adversely affect our business, financial condition, and results of operations. We may acquire or invest in other companies or technologies in the future, which could divert management’ s attention, fail to meet our expectations, result in additional dilution to our stockholders, increase expenses, disrupt our operations, or otherwise harm our operating results. We may in the future acquire or invest in ~~businesses, products, or technologies that we believe could complement or expand our platform, enhance our technical capabilities, or otherwise offer growth opportunities.~~ **We may not be able to fully realize the anticipated benefits of any future acquisitions or anticipated benefits may not transpire.** The pursuit of potential acquisitions may divert the attention of management and cause us to incur various expenses related to identifying, investigating, and pursuing suitable acquisitions, whether or not they are consummated. **Even if they are consummated, we may not be able to fully realize the anticipated benefits of any future acquisitions or anticipated benefits may not transpire.** There are inherent risks in integrating and managing acquisitions. If we acquire additional businesses, we may not be able to assimilate or integrate the acquired personnel, operations, products, services, and technologies successfully or effectively manage the combined business following the acquisition and our management may be distracted from operating our business. We also may not achieve the anticipated benefits from the acquired business due to a number of factors, including, without limitation: • unanticipated costs or liabilities associated with the acquisition; • incurrence of acquisition- related costs, which would be recognized as a current period expense; • inability to generate sufficient revenue to offset acquisition or investment costs; • inability to maintain relationships with customers and partners of the acquired business; • difficulty of incorporating acquired technology and rights into our platform and of maintaining quality and security standards consistent with our brand; • delays in customer purchases due to uncertainty related to any acquisition; • the potential loss of key employees; • use of resources that are needed in other parts of our business and diversion of management and employee resources; • inability to recognize acquired deferred revenue in accordance with our revenue recognition policies; and • use of substantial portions of our available cash and equity or the incurrence of debt to consummate the acquisition. Acquisitions also increase the risk of unforeseen legal liability, including ~~for~~ potential shareholder suits or potential violations of applicable law or industry rules and regulations, arising from prior or ongoing acts or omissions by the acquired businesses that are not discovered by due diligence during the acquisition process or new regulatory restrictions at the federal, state, or local levels. Generally, if an acquired business fails to meet our expectations, our operating results, business, and financial condition may suffer. Acquisitions could also result in dilutive issuances of equity securities or the incurrence of debt, which could adversely affect our business, results of operations and financial condition. In addition, a significant portion of the purchase price of companies ~~it we acquires~~

acquire may be allocated to goodwill and other intangible assets, which must be assessed for impairment at least annually. If our acquisitions do not ultimately yield expected returns, we may be required to take charges to our operating results based on our impairment assessment process, which could harm our results of operations. Our intellectual property rights are valuable and any inability to protect our proprietary technology and intellectual property rights could substantially harm our business and operating results. Our future success and competitive position depend in part on our ability to protect our intellectual property and proprietary technologies. To safeguard these rights, we rely on a combination of patent, trademark, copyright, and trade secret laws and contractual protections in the United States and other jurisdictions, all of which provide only limited protection and may not now or in the future provide us with a competitive advantage. We maintain a program of identifying technology appropriate for patent protection. Our practice is to require employees and consultants to execute non-disclosure and proprietary rights agreements upon commencement of employment or consulting arrangements. These agreements acknowledge our exclusive ownership of all intellectual property developed by the individuals during their work for us and require that all proprietary information disclosed will remain confidential. Such agreements may not be enforceable in full or in part in all jurisdictions and any breach could have a negative effect on our business and our remedy for such breach may be limited. We own or co-own ~~seven~~ **eight** issued U. S. patents and ~~thirteen~~ **24** issued foreign patents and have ~~fifteen~~ **24** pending or allowed patent applications relating to our products. It cannot be certain that any patents will issue from any patent applications, that patents that issue from such applications will give us the protection that we seek or that any such patents will not be challenged, invalidated, or circumvented. Any patents that may issue in the future from our pending or future patent applications may not provide sufficiently broad protection and may not be enforceable in actions against alleged infringers. We have registered the Evolv **Technology** ®, **Evolv Express** ®, **Evolv Insights**, **Evolv Cortex AI**, and Evolv Edge ® names and logos in the United States and certain other countries. We also have registrations and / or pending applications for additional marks in the United States and other countries; however, we cannot be certain that any future trademark registrations will be issued for pending or future applications or that any registered trademarks will be enforceable or provide adequate protection of our proprietary rights. We also license software from third parties for integration into our products, including open source software and other software available on commercially reasonable terms. We cannot be certain that such third parties will maintain such software or continue to make it available. If we are unable to maintain sufficient intellectual property protection for our proprietary technologies or if the scope of the intellectual property protection obtained is not sufficiently broad, our competitors and other third parties could develop and commercialize technologies similar or identical to ours, and our ability to successfully commercialize our technologies may be impaired. While we take steps to protect our intellectual property, the steps we take may be inadequate to prevent infringement, misappropriation, or other violations of our intellectual property rights. We will not be able to protect our intellectual property if we are unable to enforce our rights or if we do not detect unauthorized use of our intellectual property. Any of our patents or other intellectual property rights may be challenged by others or invalidated through administrative process or litigation. Furthermore, legal standards relating to the validity, enforceability, and scope of protection of intellectual property rights are uncertain. Some license provisions protecting against unauthorized use, copying, transfer, and disclosure of our offerings may be unenforceable under the laws of certain jurisdictions and foreign countries. In addition, the laws of some countries do not protect proprietary rights to the same extent as the laws of the United States, and mechanisms for enforcement of intellectual property rights in some foreign countries may be inadequate. Changes in the law or adverse court rulings may also negatively affect our ability to prevent others from using our technology. To the extent we expand our international activities, our exposure to unauthorized copying and use of our technology and proprietary information may increase. We may be required to spend significant resources to monitor and protect our intellectual property rights. From time to time, legal action by us may be necessary to enforce our patents and other intellectual property rights, to protect our trade secrets, to determine the validity and scope of the intellectual property rights of others or to defend against claims of infringement or invalidity. Such litigation could result in substantial costs and diversion of resources and could negatively affect our business, operating results, and financial condition. Furthermore, our efforts to enforce our intellectual property rights may be met with defenses, counterclaims, and countersuits attacking the validity and enforceability of our intellectual property rights. Our inability to protect our proprietary technology against unauthorized copying or use, as well as any costly litigation, could delay further sales or the implementation of our products and offerings, impair the functionality of our products and offerings, delay introductions of new features or enhancements, result in our substituting inferior or more costly technologies into our products and offerings, or injure our reputation. Assertions by third parties of infringement or other violations by us of their intellectual property rights, whether or not correct, could result in significant costs and harm **to** our business and operating results. Third parties may in the future assert claims of infringement, misappropriation, or other violations of intellectual property rights against us. They may also assert such claims against our customers or reseller partners, whom we typically indemnify against claims that our products infringe, misappropriate, or otherwise violate the intellectual property rights of third parties. If we do infringe a third party's rights and are unable to provide a sufficient workaround, we may need to negotiate with holders of those rights to obtain a license to those rights or otherwise settle any infringement claim as a party that makes a claim of infringement against us may obtain an injunction preventing us from shipping products containing the allegedly infringing technology. As the number of products and competitors in our market increase and overlaps occur, claims of infringement, misappropriation, and other violations of intellectual property rights may increase. Any claim of infringement, misappropriation, or other violation of intellectual property rights by a third party, even those without merit, could cause us to incur substantial costs defending against the claim and could distract our management from our business. Future assertions of patent rights by third parties, and any resulting litigation, may involve patent holding companies or other adverse patent owners who have no relevant product revenues and against whom our own patents may therefore provide little or no deterrence or protection. There can be no assurance that we will not be found to infringe or otherwise violate any third-party intellectual property rights or to have done so in the past. An adverse outcome of a dispute may require us to: • pay substantial damages, including treble damages, if we are

found to have willfully infringed a third party's patents or copyrights; • make substantial payments for legal fees, settlement payments or other costs or damages; • cease selling, making, licensing, or using products that are alleged to infringe or misappropriate the intellectual property of others; • expend additional development resources to attempt to redesign our products or otherwise develop non-infringing technology, which may not be successful; • enter into potentially unfavorable royalty or license agreements to obtain the right to use necessary technologies or intellectual property rights; • take legal action or initiate administrative proceedings to challenge the validity and scope of the third-party rights or to defend against any allegations of infringement; and • indemnify our partners and other third parties. In addition, royalty or licensing agreements, if required or desirable, may be unavailable on terms acceptable to us, or at all, and may require significant royalty payments and other expenditures. Some licenses may also be non-exclusive, and therefore our competitors may have access to the same technology licensed to us. Any of the foregoing events could seriously harm our business, financial condition, and results of operations. Even if the claims do not result in litigation or are resolved in our favor, these claims, and the time and resources necessary to resolve them, could divert the resources of our management and harm our business and operating results. Moreover, there could be public announcements of the results of hearings, motions, or other interim proceedings or developments and if securities analysts or investors perceive these results to be negative, it could have a substantial adverse effect on the price of our ordinary shares. We expect that the occurrence of infringement claims is likely to grow as the market for our products and solutions grows. Accordingly, our exposure to damages resulting from infringement claims could increase and this could further exhaust our financial and management resources. Confidentiality arrangements with employees and others may not adequately prevent disclosure of trade secrets and other proprietary information. We have devoted substantial resources to the development of our technology, business operations, and business plans. In order to protect our trade secrets and proprietary information, we rely in significant part on confidentiality arrangements with our employees, licensees, independent contractors, advisors, suppliers, reseller partners, and customers. However, we cannot guarantee that we have entered into such agreements with each party that may have or has had access to our trade secrets or proprietary technology and processes. Further, despite these efforts, these arrangements may not be effective to prevent disclosure of confidential information, including trade secrets, and may not provide an adequate remedy in the event of unauthorized disclosure of confidential information. Unauthorized parties may also attempt to copy or reverse engineer certain aspects of our technologies that we consider proprietary. In addition, if others independently develop equivalent knowledge, methods, and know-how, we would not be able to assert trade secret rights against such parties. Monitoring unauthorized uses and disclosures is difficult, and we do not know whether the steps we have taken to protect our proprietary information will be effective. Moreover, policing unauthorized use of our technologies, trade secrets and intellectual property and enforcing a claim that a party illegally disclosed or misappropriated a trade secret are difficult, expensive, time-consuming, and the outcome is unpredictable. In addition, effective trade secret protection may not be available in every country in which our products are available or where we have employees or independent contractors as some courts inside and outside the United States are less willing or unwilling to protect trade secrets. If any of our trade secrets were to be disclosed to or independently developed by a competitor or other third party, our competitive position would be materially and adversely harmed. The loss of trade secret protection could make it easier for third parties to compete with our products by copying functionality. In addition, any changes in, or unexpected interpretations of, the trade secret and employment laws in any country in which we operate may compromise our ability to enforce our trade secret and intellectual property rights. Costly and time-consuming litigation could be necessary to enforce and determine the scope of our proprietary rights, and failure to obtain or maintain trade secret protection could adversely affect our competitive business position. Our products and services may be affected from time to time by design and manufacturing defects that could adversely affect our business and result in harm to our reputation. Our touchless security screening systems are complex and may contain undetected defects or errors when first introduced or as enhancements are released that, despite testing, are not discovered until after a product has been used. This could result in delayed market acceptance of those products or claims from resellers, customers, or others, which may result in litigation, increased end user warranty, support and repair or replacement costs, damage to our reputation and business, or significant costs and diversion of support and engineering personnel to correct the defect or error. We **have been in the past and** may from time to time become subject to warranty or product liability claims related to product quality issues that could lead us to incur significant expenses. ~~Evolve~~ ~~We attempt~~ ~~attempt~~ to include provisions in our agreements with customers that are designed to limit our exposure to potential liability for damages arising from defects or errors in our products. However, it is possible that these limitations may not be effective as a result of unfavorable judicial decisions or applicable laws in existence or enacted in the future. The sale and support of our products entails the risk of product liability claims. Any product liability claim brought against ~~it us~~, regardless of its merit, could result in material expense, diversion of management time and attention, damage to our business and reputation and brand, and cause us to fail to retain existing customers or to fail to attract new customers. If the general level of physical threats / attacks declines, or is perceived by our current or potential customers to have declined, our business could be harmed. Our business is substantially dependent on enterprises and governments recognizing that mass shootings, terrorist attacks and similar security threats are not necessarily effectively prevented by conventional security products such as walk-through metal detectors. High visibility attacks on prominent enterprises and governments have increased market awareness of the problem of security threats and help to provide an impetus for enterprises and governments to devote resources to protecting against security threats, such as testing our products, purchasing them and broadly deploying them within their organizations. If security threats were to decline, or enterprises or governments perceived that the general level of security threats has declined, our ability to attract new customers and expand sales of our products to existing customers could be materially and adversely affected. A reduction in the **security** threat landscape could increase our sales cycles and harm our business, results of operations, and financial condition. If we are unable to compete effectively with new entrants and other potential competitors, our sales and profitability could be adversely affected. The sales prices for our products and services may decline for a variety of reasons, including competitive pricing pressures, discounts, a change in our mix of products and services,

anticipation of the introduction of new products or promotional programs. Competition continues to increase in the market segments in which we participate, and we expect competition to further increase in the future, thereby leading to increased pricing pressures. Larger competitors with more diverse product and service offerings may reduce the price of products that compete with theirs or may bundle them with other products and services. Additionally, currency fluctuations in certain countries and regions may negatively impact prices that partners and customers are willing to pay in those countries and regions. We cannot be certain that we will be successful in developing and introducing new products with enhanced functionality on a timely basis, or that our new product offerings, if introduced, will enable it to maintain our prices and gross profits at levels that will allow us to maintain positive gross margins and achieve profitability. Because our products may collect and store visitor and related information and images, domestic and international privacy and ~~cyber security~~ ~~cybersecurity~~ concerns, and other laws and regulations, could result in additional costs and liabilities to us or inhibit sales of our products. **In the ordinary course of our business, we and our third- party vendors collect and store personal information about individuals such as our customers and employees, as well as our proprietary business information and intellectual property and that of our customers and employees. Additionally, we rely on third parties and their security procedures for the secure storage, processing, maintenance, and transmission of information that is critical to our operations.** We and our third- party vendors may be affected by cyber- attacks and other means of gaining unauthorized access to our products, systems, and data. **Our reliance on ever- evolving** ~~For instance, cyber criminals or insiders may target us or third parties with which we have business relationships to obtain data, or in a manner that disrupts our operations or compromises our products or the systems into which our products are integrated.~~ The evolution of technology systems introduces ever more complex security risks that are difficult to predict and defend against. An increasing number of companies, including those with significant online operations, have recently disclosed breaches of their security, some of which involved sophisticated tactics and techniques allegedly attributable to criminal enterprises or nation- state actors. **While Cybersecurity threats as well as the tools (including artificial intelligence) used to breach security safeguards, circumvent security controls, evade detection, and remove forensic evidence, are also constantly evolving and may originate from remote areas increasing the difficulty of detecting and successfully defending against them.** For instance, cyber criminals or insiders may target us or third parties with which ~~we take~~ ~~we have~~ ~~business relationships to obtain data, or in a manner that disrupts our operations or compromises our products or the systems into which our products are integrated.~~ Remote and hybrid working arrangements also increase cybersecurity risks due to the challenges associated with managing remote computing assets and security vulnerabilities that are present in many non- corporate and home networks. As such, we and our third- party vendors may be subject to boycotts, spam, spyware, ransomware, phishing and social engineering, viruses, worms, malware, DDOS attacks, password attacks, impersonation of employees or officers, and other threats. Cybersecurity incidents directed at us or our third- party vendors can range from errors on the part of our personnel to uncoordinated individual attempts to gain unauthorized access to information technology systems to sophisticated and targeted measures known as advanced persistent threats. Specifically, a cyber incident could be caused by disasters, insiders (through inadvertence or with malicious intent), or malicious third parties (including nation- states or nation- state supported actors) using sophisticated, targeted methods ~~to protect~~ ~~circumvent~~ ~~firewalls, encryption, and the other~~ security defenses of personal information-, **including hacking, fraud, trickery, or other forms of deception.** And it is possible that our security controls over personal information and other practices we follow may not prevent the unauthorized access to, or the unintended release of, personal information. In addition, we do not know whether our current practices will be deemed sufficient under applicable laws or whether new regulatory requirements might make our current practices insufficient. ~~parties and their security procedures for the secure storage, processing, maintenance, and transmission of information that is critical to our operations.~~ Despite measures designed to prevent, detect, address, and mitigate cybersecurity incidents, such **measures will require updates and improvements, and we cannot guarantee that such measures will be adequate to detect, prevent or mitigate cyber incidents.** Such incidents may occur to us or our third- party providers and, depending on their nature and scope, could potentially result in the misappropriation, destruction, corruption or unavailability of critical data and confidential or proprietary information (our own or that of third parties, including personal information of our customers and employees) and the disruption of business operations. ~~We~~ ~~If~~ ~~there~~ ~~is~~ ~~a~~ ~~breach~~ ~~of~~ ~~our~~ ~~computer~~ ~~systems~~ ~~and~~ ~~we~~ ~~know~~ ~~or~~ ~~suspect~~ ~~that~~ ~~certain~~ ~~personal~~ ~~information~~ ~~has~~ ~~been~~ ~~accessed,~~ ~~or~~ ~~used~~ ~~inappropriately,~~ we may need to inform the affected individual and may be subject to significant fines and penalties. In the event of a breach, we could face government scrutiny or consumer class actions. **Furthermore, there can be no assurance that our** ~~Cybersecurity~~ ~~cybersecurity~~ ~~incidents~~ ~~directed~~ ~~at~~ ~~us~~ **risk management program and processes, including or our policies, controls, or procedures, will be fully implemented, complied with or effective in protecting our systems and information. We and** our third- party vendors ~~can range from errors on the part.....~~ ~~the~~ ~~disruption~~ ~~of~~ ~~business~~ ~~operations.~~ We have experienced and expect to continue to experience ~~attempted routine~~ ~~cyber-~~ ~~attacks~~ ~~of~~ ~~our~~ ~~information~~ ~~technology~~ ~~networks~~-, such as through phishing scams and ransomware. Although none of these actual or attempted cyber- attacks has had a material adverse impact on our operations or financial condition, we cannot guarantee that any such incidents will not have such an impact in the future. For example, we are at risk for interruptions, outages and breaches of: operational systems, including business, financial, accounting, product development, data processing or production processes, owned by us or our third- party vendors or suppliers; facility security systems, owned by us or our third- party vendors or suppliers; in- product technology owned by us or our third- party vendors or suppliers; the integrated software in our solutions; or customer or other data that we process or our third- party vendors or suppliers process on our behalf. Such cyber incidents could materially disrupt operational systems; result in loss of intellectual property, trade secrets or other proprietary or competitively sensitive information; compromise certain information of customers, employees, suppliers, or others; jeopardize the security of our facilities; or affect the performance of in- product technology and the integrated software in our solutions. A cyber **Due to concerns about data security and integrity, a growing number of legislative and**

regulatory bodies have adopted breach notification and other requirements in the event that information subject to such laws is accessed by unauthorized persons and additional regulations regarding the use, access, accuracy, and security of such data are possible. For example, in the United States, we are subject to laws in all states and numerous territories that require notification. In addition, the SEC has recently adopted rules on the Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies that enhances and standardizes disclosures for public companies with regards to their cybersecurity risk strategy, management, and governance. Complying with such numerous and complex regulations in the event of unauthorized access would be expensive and difficult, and failure to comply with these regulations could subject us to regulatory scrutiny and additional liability. We are subject to governmental regulation and other legal obligations, particularly related to privacy, data protection and product marketing, and our actual or perceived failure to comply with such obligations could harm our business. We, our reseller partners, and our customers are subject to a number of domestic and international laws and regulations that apply to cloud services and the internet generally. These laws, rules, and regulations address a range of issues including data privacy and cyber security, breach notification and restrictions or technological requirements regarding the collection, use, storage, protection, disclosure, retention, transfer, or other processing of data. The regulatory framework for online services, data privacy and cyber security issues worldwide can vary substantially from jurisdiction to jurisdiction, is rapidly evolving and is likely to remain uncertain for the foreseeable future. Many federal, state, local, and foreign government bodies and agencies have adopted or are considering adopting laws, rules and regulations regarding the collection, use, storage, disclosure and other processing of information, web browsing and geolocation data collection, data analytics, facial recognition, cyber security, and breach response and notification procedures. Furthermore, existing laws and regulations are constantly evolving, and new laws and regulations that apply to our business are being introduced at every level of government in the United States, as well as internationally. As we seek to expand our business, we are, and may increasingly become subject to various laws, regulations, and standards, and may be subject to contractual obligations relating to data privacy and security in the jurisdictions in which we operate. Any significant change to applicable laws, regulations or industry practices, or how each is interpreted, regarding the use or disclosure of personal information, or regarding the manner in which the express or implied consent of customers for the use and disclosure of personal information is obtained, could require us to modify our products and features, possibly in a material manner and subject to increased compliance costs, which may limit our ability to develop new products and features that make use of the personal information that our customers voluntarily share. Any failure, or perceived failure, by us to comply with any federal or state privacy or security laws, regulations, industry self-regulatory principles, or codes of conduct, regulatory guidance, orders to which we may be subject, or other legal obligations relating to data privacy or security could adversely affect our reputation, brand and business, and may result in claims, liabilities, proceedings or actions against us by governmental entities, customers or others. Any such claims, proceedings or actions could hurt our reputation, brand, and business, force us to incur significant expenses in defense of such proceedings or actions, distract our management, increase our costs of doing business, result in a loss of customers and result in the imposition of monetary penalties. In the United States, there are numerous federal and state data privacy and security laws, rules, and regulations governing the collection, use, disclosure, retention, security, transfer, storage, and other processing of personal data information, including federal and state data privacy laws, data breach notification laws, and consumer protection laws. For example, the The U. S. Federal Trade Commission ("FTC") and many state attorneys general are interpreting federal and state consumer protection laws to impose standards for the online collection, use, dissemination, and security of data. Such standards require us to publish statements that describe how we handle personal data and choices individuals may have about the way we handle their personal data. If such information that we publish is considered untrue or inaccurate, we may be subject to government claims of unfair or deceptive

trade practices, which could lead to significant liabilities and consequences. Moreover, according to the FTC, violating consumers' privacy rights or failing to take appropriate steps to keep consumers' personal data secure may constitute unfair acts or practices in or affecting commerce in violation of Section 5 (a) of the Federal Trade Commission Act. State consumer protection laws provide similar causes of action for unfair or deceptive practices. There are also laws and regulations governing the collection and use of biometric information, such as fingerprints and face prints. For example, the Illinois Biometric Information Privacy Act ("BIPA") applies to the collection and use of "biometric identifiers" and "biometric information" which include finger and face prints. A business required to comply with BIPA is not permitted to sell, lease, trade or otherwise profit from biometric identifiers or biometric information it collects, and is also under obligations to have a written policy with respect to the retention and destruction of all biometric identifiers and biometric information; ensure that it informs the subject of the collection and the purpose of the collection and obtains consent for such collection; and obtain consent for any disclosure of biometric identifiers or biometric information. Individuals are afforded a private right of action under BIPA and may recover statutory damages equal to the greater of \$ 1, 000 per incident or actual damages and reasonable attorneys' fees and costs. Several class action lawsuits have been brought under BIPA, as the statute is broad and still being interpreted by the courts. Additionally, a number of other proposals exist for new federal and state privacy legislation that, if passed, could increase our potential liability, increase our compliance costs and materially adversely affect our business. To the extent that regulation of data privacy and cybersecurity continues to increase, we may incur additional compliance costs and may be exposed to increased noncompliance risk.

In addition, many state legislatures have adopted legislation that regulates how businesses operate online, including measures relating to privacy, data security, and data breaches. Such legislation includes the California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act ("CCPA-CPRPA"), which grants enhanced privacy rights for California consumers and imposes obligations on companies that process their personal information. Among other things, the CCPA gives California consumers expanded rights related to their personal information, including the right to access, correct and delete their personal information, opt out and receive detailed information about how of certain processing of their personal information is, including possibly restricting the use and shared. The CCPA also provides California consumers the right to opt-out of certain sales of personal information and may restrict the use of cookies and similar technologies for advertising purposes. The CCPA prohibits discrimination against individuals who exercise their privacy rights, and provides for civil penalties for violations enforceable by the California Attorney General as well as a private right of action for certain data breaches that result in the loss of personal information. This private right of action is expected to increase the likelihood of, and risks associated with, data breach litigation. Additionally, the California Privacy Rights Act (the "CPRPA"), which substantially amends the CCPA, went into effect on January 1, 2023 and becomes enforceable on July 1, 2023. The CPRPA restricts use of certain categories of sensitive personal information that we handle; further restricts the use of cross-context behavioral advertising techniques on which our products may rely in the future; establishes restrictions on the retention of personal information; expands the types of data breaches subject to the private right of action; and establishes the California Privacy Protection Agency to implement and enforce the new law, as well as impose administrative fines. Additionally, comprehensive privacy statutes that share similarities with the CCPA have been enacted in Virginia (effective January 1, 2023), Colorado (effective July 1, 2023), Connecticut (effective July 1, 2023), and Utah (effective December 31, 2023). These comprehensive state privacy laws may increase our compliance costs and potential liability, particularly in the event of a data breach, and could have a material adverse effect on our business, including how we use personal information, our financial condition, and the results of our operations or prospects. Similar laws have been proposed in other states and at the federal level legislation has also been enacted and / or proposed, reflecting a trend toward more stringent data privacy legislation in the United States. This legislation may add additional complexity, variation in requirements, restrictions, and potential legal risk, require additional investment in resources to compliance programs, could impact strategies and availability of previously useful data, and could result in increased compliance costs and / or changes in business practices and policies. In addition, some laws may require us to notify governmental authorities and / or affected individuals of data breaches involving certain personal information or other unauthorized or inadvertent access to or disclosure of such information. We may need to notify governmental authorities and affected individuals with respect to such incidents. For example, laws in all 50 U. S. states may require businesses to provide notice to consumers whose personal information has been disclosed as a result of a data breach. These laws are not consistent, and compliance in the event of a widespread data breach may be difficult and costly. We also may be contractually required to notify consumers or other counterparties of a security breach. Regardless of our contractual protections, any actual or perceived security breach or breach of our contractual obligations could harm our reputation and brand, expose us to potential liability or require us to expend significant resources on data security and in responding to any such actual or perceived breach. Internationally, virtually every jurisdiction in which we operate and has customers and / or have prospective customers to which we market has established its own data security and privacy legal frameworks with which we, our reseller partners or our customers must comply. Further For example, in many federal, state and foreign government bodies and agencies have introduced, and are currently considering, additional laws and regulations, including related to the development and integration of AI, machine learning, and additional emerging data technologies. If passed, we will likely incur additional expenses and costs associated with complying with such laws, as well as face heightened potential liability if we are unable to comply with these laws. In Europe and the United Kingdom ("UK"), we are subject to the European Union General Data Protection Regulation (the "EU GDPR") and to the United Kingdom General Data Protection Regulation and Data Protection Act 2018 (collectively, the "UK GDPR") (the EU GDPR and UK GDPR together referred to as the "GDPR"). The GDPR imposes comprehensive data privacy compliance obligations in relation to our collection, processing, sharing, disclosure, transfer, and other use of data relating to an identifiable living individual or "personal data," including a principal of accountability and the obligation to demonstrate compliance through policies, procedures, training, and audit. Non-compliance with the EU GDPR and UK GDPR can trigger steep fines of up to the

greater of (i) 4 % of total worldwide annual turnover and (ii) € 20 million. Separate EU and UK laws and regulations (and national implementations thereof) govern the protection of consumers and of electronic communications and these are also evolving. For instance, the current European laws that cover the use of cookies and similar technology and marketing online or by electronic means are under reform. A draft of the new ePrivacy Regulation extends the strict opt- in marketing rules with limited exceptions to business- to- business communications, alters rules on third- party cookies, web beacons and similar technology and significantly increases penalties. We cannot yet determine the impact such future laws, regulations, and standards may have on our business. Such laws and regulations are often subject to differing interpretations and may be inconsistent among jurisdictions. Compliance with the EU GDPR and UK GDPR, and other such laws, may incur substantial expense and we may be required to make significant changes in our business operations and product and services development, all of which may adversely affect our revenues and our business. We are also subject to EU and UK ~~and~~ rules with respect to cross- border transfers of personal data out of the **European Economic Area (the " EEA ")** and the UK, respectively. Recent legal developments in Europe have created complexity and uncertainty regarding transfers of personal data from the EEA and the UK to the United States. ~~On July 16, 2020, the Court of Justice of the European Union (" CJEU ") invalidated the EU- US Privacy Shield Framework (" Privacy Shield ") under which personal data could be transferred from the EEA to US entities who had self- certified under the Privacy Shield scheme. The CJEU further noted that reliance on the standard contractual clauses (a standard form of contract approved by the European Commission as an adequate personal data transfer mechanism, and potential alternative to the Privacy Shield) alone may not necessarily be sufficient in all circumstances and that transfers~~ **Transfers** must be assessed on a case- by- case basis **and reliance on the standard contractual clauses (a standard form of contract approved by the European Commission as an adequate personal data transfer mechanism,) alone may not necessarily be sufficient in all circumstances**. European court and regulatory decisions ~~subsequent to the CJEU decision of July 16, 2020 have taken~~ **take** a restrictive approach to international data transfers. The UK regulator has adopted a similar approach to data export outside of the UK and, on March 21, 2022, the international data transfer agreement and the international data transfer addendum to the European Commission' s standard contractual clauses for international data transfers came into force. The UK regulator also recommends, consistent with the European Commission approach, a transfer risk assessment is undertaken. Use of such standard contractual clauses must now be assessed on a case- by- case basis taking into account the legal regime applicable in the destination country, in particular applicable surveillance laws and rights of individuals and additional measures and / or contractual provisions may need to be put in place, however, the nature of these additional measures is currently uncertain. As the enforcement landscape further develops, and supervisory authorities issue further guidance on international data transfers, we could suffer additional costs, complaints and / or regulatory investigations or fines; we may have to stop using certain tools and vendors and make other operational changes and / or it could otherwise affect the manner in which we provide our services, and could adversely affect our business, operations, and financial condition.

~~circumstances~~. **Separately, there are increasing concerns regarding how AI and safeguards must be implemented to safeguard individual rights- machine learning can result in unintentional bias or discrimination**, including **on** the right to obtain human intervention **basis of race, ethnicity, gender, or other protected classes. Regulators and other governmental bodies are increasingly focused on mitigating or controlling for bias** to contest any decision. ~~If passed, we will likely incur additional expenses and~~ **discrimination in** costs associated with complying with such laws, as well as ~~face heightened potential liability if we are unable to comply with these~~ **the laws context of AI and machine learning**. While we minimize any physical bias in our product' s identification of threats because the product' s AI does not process or analyze ~~an individual~~ **individuals' s** physical characteristics, we may not be able to identify such issues in advance, or if identified, we may not be able to identify mechanisms for effectively mitigating such issues We strive to comply with all applicable laws, policies, legal obligations, and industry codes of conduct relating to privacy and data protection to the extent possible. Because the interpretation and application of privacy and data protection laws are still uncertain, it is possible that these laws may be interpreted and applied in a manner that is inconsistent from one jurisdiction to another or with our existing practices or the features of our products and may conflict with other rules or regulations, making enforcement, and thus compliance requirements, ambiguous, uncertain, and potentially inconsistent. Any **significant change to applicable laws, regulations or industry practices, or how each is interpreted, regarding the use or disclosure of personal information, or regarding the manner in which the express or implied consent of customers for the use and disclosure of personal information is obtained, could require us to modify our products and features, possibly in a material manner and subject to increased compliance costs, which may limit our ability to develop new products and features that make use of the personal information that our customers voluntarily share. Any** failure or perceived failure by us to comply with our privacy policies, privacy- related obligations to customers or other third parties, or our privacy- related legal obligations, or any compromise of security that results in the unauthorized access to or unintended release of personally identifiable information or other customer data, may result in governmental enforcement actions, litigation, or public statements against us by consumer advocacy groups or others. Any of these events could cause us to incur significant costs in investigating and defending such claims and, if found liable, pay significant damages. Further, these proceedings and any subsequent adverse outcomes may cause our customers to lose trust in us, which could have an adverse effect on our reputation and business. We may also be subject to claims of liability or responsibility for the actions of third parties with whom we interact or upon whom it relies in relation to various products, including but not limited to vendors and business partners. If so, in addition to the possibility of fines, lawsuits and other claims, we could be required to fundamentally change our business activities and practices or modify our products, which could have an adverse effect on our business. Any inability to adequately address privacy and / or data concerns, even if unfounded, or comply with applicable privacy or data protection laws, regulations, and policies, could result in additional cost and liability to us, damage our reputation, inhibit sales and adversely affect our business. ~~Separately, there are increasing concerns.....~~ **identify mechanisms for effectively mitigating such issues**. The costs of compliance with, and other burdens imposed by, the laws, rules, regulations, and policies that are

applicable to the businesses of our customers may limit the use and adoption of, and reduce the overall demand for, our software. Even the perception of privacy or discrimination concerns, whether or not valid, may harm our reputation, inhibit adoption of our products by current and future customers, or adversely impact our ability to attract and retain workforce talent. Our failure to comply with applicable laws and regulations, or to protect such data, could result in enforcement action against us, including fines, imprisonment of company officials and public censure, claims for damages by customers and other affected individuals, damage to our reputation and loss of goodwill (both in relation to existing customers and prospective customers), any of which could have a material adverse effect on our operations, financial performance and business. We may also have costs associated with engaging with stakeholders, including investors, insurance providers, and other capital providers, on such issues.

The marketing and sale of our products are also subject to extensive regulation by various federal agencies, including the FTC and Customer Product Safety commission, as well as various other federal, state, provincial, local, and international regulatory authorities in the countries in which our products are distributed or sold and industry codes of conduct. From time to time, we receive government regulatory inquiries and requests for information relating to our marketing practices and our approach is to be cooperative and educate them about our company and products. For example, the FTC has requested information about certain aspects of our marketing practices. We are complying with the FTC's requests and have been cooperating with them to answer their questions and educate them about our mission. Furthermore, in February 2024, we received a subpoena from the SEC, Division of Enforcement, requesting that we produce certain documents and information, much of which is similar to the documents and information previously requested by the FTC. We are cooperating and intend to continue to cooperate with the SEC's investigation. The Company is cooperating with the FTC and SEC with respect to the investigations, and there can be no assurance whether there will be further information requests or potential enforcement or litigation, which is necessarily uncertain. We can offer no assurances as to the outcome of these investigations or their potential effect, if any, on us or our results of operations. Any inability to adequately address the FTC's or SEC's concerns, even if unfounded, or comply with applicable laws, regulations, and policies, could result in enforcement actions or significant penalties or claims, which could, in turn, divert financial and management resources, damage our reputation, inhibit sales, and otherwise adversely affect our business. In addition to the possibility of fines, injunctive relief, lawsuits and other claims, we could be required to fundamentally change our business operations, marketing activities, and practices. Responding to these or other investigations alone can be costly and time-consuming. Regulations related to "conflict minerals" may force us to incur additional expenses, may result in damage to our business reputation and may materially and adversely impact our ability to conduct our business. As a public company, we are subject to the requirements under the Dodd- Frank Wall Street Reform and Consumer Protection Act of 2010 (the "Dodd- Frank Act") that require us to exercise diligence, disclose and report whether or not our devices contain conflict minerals. These requirements could adversely affect the sourcing, availability and pricing of the materials used in the manufacture of components used in our devices. In addition, we will incur additional costs to comply with the disclosure requirements, including costs related to conducting diligence procedures to determine the sources of conflict minerals that may be used or necessary to the production of our devices and, if applicable, potential changes to devices, processes or sources of supply as a consequence of such verification activities. It is also possible that we may face reputational harm if we determine that certain of our devices contain minerals which are not determined to be conflict-free or if we are unable to alter our devices, processes, or sources of supply to avoid such materials.

Our operating results may be harmed if we are required to collect sales and use or other related taxes for our products in jurisdictions where it has not historically done so. Taxing jurisdictions, including state, local, and foreign taxing authorities, have differing rules and regulations governing sales and use or other taxes, and these rules and regulations are subject to varying interpretations that may change over time. In particular, significant judgment is required in evaluating our tax positions and our worldwide provision for taxes. While we believe that we are in material compliance with our obligations under applicable taxing regimes, one or more states, localities, or countries may seek to impose additional sales or other tax collection obligations on us, including for past sales by us or our reseller partners. It is possible that we could face sales tax audits and that such audits could result in tax-related liabilities for which it has not accrued. A successful assertion that it should be collecting additional sales or other taxes on our products in jurisdictions where it has not historically done so and do not accrue for sales taxes could result in substantial tax liabilities for past sales, discourage customers from purchasing our products or otherwise harm our business and operating results. In addition, our tax obligations and effective tax rates could be adversely affected by changes in the relevant tax, accounting and other laws, regulations, principles and interpretations (such as the recent United States Inflation Reduction Act which, among other changes, introduced a 15 % corporate minimum tax on certain United States corporations and a 1 % excise tax on certain stock redemptions by United States corporations), including those relating to income tax nexus, jurisdictional mix of profits at varying statutory tax rates, by changes in foreign currency exchange rates, or by changes in the valuation of our deferred tax assets and liabilities. Although we believe our tax estimates are reasonable, the final determination of any tax audits or litigation could be materially different from our historical tax provisions and accruals, which could have a material adverse effect on our operating results or cash flows in the period or periods for which a determination is made. For example, in 2021 we established a new wholly owned subsidiary of Evolv Technologies Holdings, Inc., Give Evolv LLC, a Delaware limited liability company, to (1) promote our core mission in locations that might not otherwise be able to afford our weapons detection security screening systems and related products and services, (2) make public venues and institutions safer for all patrons, students, visitors, and other attendees, and (3) carry out charitable efforts consistent with the foregoing mission, for which historical tax data does not exist. Our ability to utilize net operating loss carryforwards as well as research and development tax credit carryforwards to offset future taxable income may be subject to certain limitations and we could be subject to tax audits or examinations that could result in a loss of our net operating loss carryforwards as well as research and development credits and / or cash tax exposures. As of December 31, 2023

and 2022 and 2021, we had gross federal net operating losses of \$ 20. 1 million and \$ 20. 1 million that are subject to expire at various dates beginning in 2033, and federal net operating losses of \$ 142. 4 million and \$ 124. 3 million and \$ 79. 7 million, which have no expiration date and can be used to offset up to 80 % of future taxable income in any one tax period, respectively. We also had gross state net operating loss carryforwards of \$ 142. 4 million and \$ 103 . 8 million and \$ 75. 8 million for the years ended December 31, 2023 and 2022 and 2021, respectively, which may be available to offset future state taxable income and which begin to expire in 2033. Additionally, as of December 31, 2022 and 2021, we had no gross UK United Kingdom net operating loss carryforwards as of December 31, 2023 and gross UK net operating loss carryforwards of approximately \$ 2. 3 million and \$ 1. 5 million, respectively, that will not expire as . As of December 31, 2022 . As of December 31, 2023 , we had gross U. S. federal and state research and development and other tax credit carryforwards of \$ 2. 5 million and \$ 1. 6 million, respectively, which may be available to offset future tax liabilities and the majority of which begin to expire in 2033 and 2029 2030 , respectively. As of December 31, 2021-2022 , we had gross U. S. federal and state research and development and other tax credit carryforwards of \$ 3-2 . 3-5 million and \$ 2-1 . 6 million, respectively, which may be available to offset future tax liabilities and the majority of which begin to expire in 2033 and 2029, respectively. These net operating loss and tax credit carryforwards could expire unused and be unavailable to offset our future income tax liabilities. In addition, under Section 382 of the Internal Revenue Code of 1986, as amended, or the Code, and corresponding provisions of state law, if a corporation undergoes an “ ownership change, ” which is generally defined as a greater than 50 % change, by value, in our equity ownership over a three- year period, the corporation’ s ability to use our pre- change net operating loss carryforwards and other pre- change tax attributes to offset our post- change income may be limited. We have not determined if we have experienced Section 382 ownership changes as of December 31, 2022-2023 and if a portion of our net operating loss and tax credit carryforwards is subject to an annual limitation under Section 382. In addition, we may experience ownership changes in the future as a result of subsequent shifts in our stock ownership, some of which may be outside of our control, but that would not be material to the consolidated financial statements for the year ended December 31, 2022-2023 . If we determine that an ownership change has occurred and our ability to use our historical net operating loss and tax credit carryforwards is materially limited, it would harm our future operating results by effectively increasing our future tax obligations. Our cash and cash equivalents could be adversely affected if the financial institutions at which we hold our cash and cash equivalents fail. We maintain the majority Market conditions impacting financing institutions could impact our ability to access some or all of our cash , and cash equivalents and marketable securities, and we may be unable to obtain alternative funding when and as needed and on acceptable terms, if at all. The performance of the capital markets affects the values of funds that are held in marketable securities. These assets are subject to market fluctuations and various developments, including, without limitation, rating agency downgrades that may impair their value. Further, a bankruptcy of one of the banks in which or through which we hold or invest our cash reserves, might prevent us from accessing all or a portion of that cash for an uncertain period of time if at all. We maintain substantially all of our cash and cash equivalents in accounts with major U. S. and multi- national financial institutions, including Silicon Valley Bank (“ SVB”), and our deposits at certain of these institutions exceed insured limits. Market conditions can impact the viability of these institutions. In the event of a future failure For or example, on March 10, 2023, SVB was closed. closure by of any of the financial institutions where we maintain our cash and cash equivalents, the there California can be no assurance that we would be able to access uninsured funds in a timely manner or at all, and there is no guarantee that the Federal Reserve Board, the U. S. Treasury Department of Financial Protection and Innovation, which appointed the Federal Deposit Insurance Corporation (“ FDIC”) as receiver. The FDIC created a successor bridge bank, Silicon Valley Bridge Bank, N. A. (“ SVBB ”), and all deposits of SVB were transferred to SVBB under a systemic risk exception approved by the Federal Reserve, the U. S. Treasury Department, and the FDIC. While the Federal Reserve, the U. S. Treasury Department, and the FDIC announced in a joint statement on March 12, 2023 that all SVB deposits, including both insured and uninsured amounts, would be available in full to account holders, a similar failure of any of the financial institutions where we maintain our cash and cash equivalents could impact our ability to access uninsured funds in a timely manner or at all. There is no guarantee that the Federal Reserve Board, the U. S. Treasury Department and the FDIC will provide access to uninsured funds in the future in the event of the closure of any other banks or financial institutions in a timely fashion or at all. Any inability to access or delay in accessing these funds could adversely affect our ability to finance our operations, which, in turn, could adversely affect our business , results of operations , financial position, and liquidity. If we do not effectively diversify our bank deposits and investment portfolio, the value and liquidity of our investments may fluctuate substantially which could affect our access to capital and results of operations in a material way. Furthermore, our access to our cash and cash equivalents in amounts adequate to finance our operations could be significantly impaired if the financial institutions with which we have arrangements directly face liquidity constraints or failures. Investor concerns regarding the U. S. or international financial systems could result in less favorable commercial financing terms, including higher interest rates or costs and tighter financial and operating covenants, or systemic limitations on access to credit and liquidity sources, thereby making it more difficult for us to acquire financing on acceptable terms or at all. Any material decline in available funding or our ability to access our cash and cash equivalents could adversely impact our results of operations and liquidity. We may require additional capital to support business growth, and this capital might not be available on acceptable terms, if at all. We intend to continue to make investments to support our business growth and may require additional funds to respond to business challenges, including the need to develop new features or enhance our products, improve our operating infrastructure, or acquire complementary businesses and technologies. Accordingly, we may need to engage in equity or debt financings to secure additional funds. If we raise additional funds through future issuances of equity or convertible debt securities, our existing stockholders could suffer significant dilution, and any new equity securities we issue could have rights, preferences , and privileges superior to those of holders of our common stock. Any debt financing that we may secure in the future could involve restrictive covenants relating to our capital raising activities and other financial and operational matters, which may make it

more difficult for us to obtain additional capital and to pursue business opportunities, including potential acquisitions. We may not be able to obtain additional financing on terms favorable to it, if at all. If we are unable to obtain adequate financing or financing on terms satisfactory to it when we require it, our ability to continue to support our business growth and to respond to business challenges could be significantly impaired, and our business may be adversely affected. We face risks related to our indebtedness. As of December 31, 2022, we had total outstanding debt of \$ 29.7 million under our Credit Agreement with SVB (“2022 SVB Credit Agreement”), as amended. In connection with the closure of SVB on March 10, 2023 and the creation of SVBB, SVBB assumed all loans that were previously held by SVB. SVBB continues to hold the Company’s term loans under the same existing terms and covenants which were in place with SVB. Subject to the limits contained in the 2022 SVB Credit Agreement, we may incur additional indebtedness in the future. Our leverage (including additional indebtedness that we might incur in the future) could have important consequences to us, including: • exposing us to the risk of increased interest rates as our borrowings under our current debt facilities are at (and any borrowings in the future might be at) variable rates; • making it more difficult for us to make payments on our debt; • limiting our ability to pay future dividends; • increasing our vulnerability to downturns in our business, the security screening industry or the general economy and limiting our flexibility in planning for, or reacting to, changes in our business; • requiring a substantial portion of cash flow from operations to be dedicated to the payment of principal and interest on our debt, thereby reducing our ability to use our cash flow to fund our operations, capital expenditures, and future business opportunities; • restricting us from making strategic acquisitions or causing us to make non-strategic divestitures; • requiring us to comply with financial and operational covenants as well as liquidity and leverage covenants, restricting us, among other things, from placing liens on our assets, making investments, incurring debt, making payments to our equity or debt holders and engaging in transactions with affiliates; • limiting our ability to obtain additional debt or equity financing for working capital, capital expenditures, business development, product development, debt service requirements, acquisitions, and general corporate or other purposes; • preventing us from taking advantage of business opportunities as they arise or successfully carrying out our plans to expand our product offerings; and • placing us at a competitive disadvantage compared to our competitors who may be less leveraged. Consequences of the indebtedness that we have borrowed (and any indebtedness that we might borrow in the future) may require a substantial portion of cash flow from operations to be dedicated to the payment of principal and interest on our debt, thereby reducing our ability to use our cash flow to fund operations, capital expenditures, and future business opportunities. If we cannot generate sufficient cash flow from operations to service our debt, we may need to refinance our debt, dispose of assets or issue equity to obtain necessary funds. We do not know whether we would be able to take any of these actions on a timely basis, on terms satisfactory to us, or at all. Further, our ability to issue additional debt could be adversely affected by other factors, including market conditions. The failure by us or our subsidiaries to comply with financial covenants or other restrictions contained in the agreements governing our indebtedness could result in an event of default under such indebtedness, which could adversely affect our ability to respond to changes in our business and manage our operations and could further exacerbate the risks to our financial condition described above. Upon the occurrence of an event of default under any of the agreements governing our indebtedness, the lenders could elect to declare all amounts outstanding to be due and payable and exercise other remedies as set forth in the agreements. If any of our indebtedness were to be accelerated, there can be no assurance that our assets would be sufficient to repay this indebtedness in full, which could have a material adverse effect on our ability to continue to operate as a going concern. We have identified material weaknesses in our internal control over financial reporting and **our internal control over financial reporting was not effective as of December 31, 2023. We** may identify additional material weaknesses in the future or otherwise fail to maintain effective internal control over financial reporting, which may result in a material misstatement of our consolidated financial statements or cause us to fail to meet our periodic reporting obligations. **We As described in Part II, Item 9A – Controls and Procedures, of this Annual Report on Form 10-K, we** have identified material weaknesses in our internal control over financial reporting. A material weakness is a deficiency, or combination of deficiencies, in internal control over financial reporting such that there is a reasonable possibility that a material misstatement of the annual or interim consolidated financial statements will not be prevented or detected on a timely basis. We did not design and maintain an effective control environment commensurate with our financial reporting requirements. Specifically, we lacked a sufficient complement of personnel with an appropriate level of internal controls and accounting knowledge, training and experience commensurate with our financial reporting requirements. Additionally, the limited personnel resulted in our inability to consistently establish appropriate authorities and responsibilities in pursuit of our financial reporting objectives, as demonstrated by, among other things, insufficient segregation of duties in our finance and accounting functions. **This In addition, we did not design and maintain effective controls in response to the risks of material misstatement, as changes to existing controls or the implementation of new controls were not sufficient to respond to changes to the risks of material misstatement to the financial reporting. These material weakness weaknesses** contributed to the following additional material weaknesses: • We did not design and maintain effective controls over the period-end financial reporting process to achieve complete, accurate, and timely financial accounting, reporting and disclosures, including the classification of various accounts in the consolidated financial statements and the presentation and disclosure of items in the consolidated **statement statements** of cash flows. • We did not design and maintain processes and controls to analyze, account for and disclose non-routine, unusual or complex transactions. Specifically, we did not design and maintain controls to timely analyze and account for debt modifications and extinguishments, convertible notes, warrant instruments, non-routine complex revenue transactions including the leasing of products and transfer of inventory for leased assets into property plant and equipment, merger transactions, and the accounting and valuation of earn out liabilities. • We did not design and maintain formal accounting policies, procedures, and controls to achieve complete, accurate, and timely financial accounting, reporting and disclosures, including segregation of duties **and, controls to validate reliability of system-generated information used in the controls,** controls over the preparation and review of account reconciliations and journal entries. • We did not design and maintain effective controls **over** to ensure the

recording of **revenue, receivables, and deferred** revenue transactions, **in the appropriate period.** • We did not design and maintain effective controls over the completeness and accuracy of accounts payable and accrued liabilities, **commissions, equity and share-based compensation, fixed assets, inventory, payroll, income taxes, and cash and investments.** These material weaknesses resulted in audit adjustments and certain immaterial misstatements in the Evolv financial statements to prepaid and other current assets, accounts payable and accrued liabilities, long-term and short-term debt, convertible notes, contingent earn-out liabilities, change in fair value of contingent earn-out liability, equity, commission assets, contract **asset assets,** revenue, deferred revenue, accounts receivable, inventory, property plant and equipment, cost of sales and various expense line items and related financial statement disclosures as of and for the years ended December 31, 2019, 2020 and 2021. The material ~~weakness~~ **weaknesses** related to accounting for warrant instruments, the classification of various accounts in the consolidated financial statements and the presentation and disclosure of items in the consolidated ~~statement~~ **statements** of cash flows also resulted in the revision of the Company's previously issued 2020 annual financial statements, 2021 quarterly and annual financial statements, and quarterly financial statements for the three months ended March 31, 2022. ~~See Note 1 to our consolidated~~, **as well as the restatement of the Company's** financial statements **as of and** for the year **three and six months** ended ~~December 31~~ **June 30, 2022-2023** contained elsewhere in this Annual Report on Form 10-K. Additionally, these material weaknesses could result in a misstatement of substantially all of our accounts or disclosures that would result in a material misstatement to the annual or interim consolidated financial statements that would not be prevented or detected. • In addition to the foregoing, we did not design and maintain effective controls over information technology ("IT") general controls for information systems that are relevant to the preparation of our consolidated financial statements, specifically, with respect to: (i) program change management controls for financial systems to ensure that IT program and data changes affecting financial IT applications and underlying accounting records are identified, tested, authorized, and implemented appropriately; (ii) user access controls to ensure appropriate segregation of duties and that adequately restrict user and privileged access to financial applications, programs, and data to appropriate company personnel; (iii) computer operations controls to ensure that critical batch jobs are monitored and data backups are authorized and monitored, and (iv) testing and approval controls for program development to ensure that new software development is aligned with business and IT requirements. These IT deficiencies did not result in a misstatement to the consolidated financial statements, however, the deficiencies, when aggregated, could impact maintaining effective segregation of duties, as well as the effectiveness of IT-dependent controls (such as automated controls that address the risk of material misstatement to one or more assertions, along with the IT controls and underlying data that support the effectiveness of system-generated data and reports) that could result in misstatements potentially impacting all financial statement accounts and disclosures that would not be prevented or detected. Accordingly, management has determined these deficiencies in the aggregate constitute a material weakness. We have continued implementation of a plan to remediate these material weaknesses. These remediation measures are ongoing and include hiring additional accounting, internal audit, and IT personnel to bolster our reporting, technical accounting, and IT capabilities. We are in the process of designing and implementing controls to formalize roles and review responsibilities to align with our team's skills and experience and designing and implementing controls over segregation of duties. We ~~have engaged outside consultants to assist us in these efforts.~~ We added, and continue to add, finance personnel, including a Chief Financial Officer and a Chief Accounting Officer, to strengthen our internal accounting team, to provide oversight, structure and reporting lines, and to provide additional review over our disclosures. We **have performed a financial statement risk assessment in order to identify material financial statement line items for which key controls are needed in order to ensure complete and accurate financial reporting, and have engaged outside consultants to assist with the process of designing** ~~design~~ and ~~implementing~~ **implementation of control activities resulting from the risk assessment. We have designed and implemented additional review and training procedures within our accounting and finance functions to enhance knowledge and understanding of internal control over financial reporting. During each of the three months ended June 30, September 30, and December 31, 2023, we implemented** controls related to, **among other items,** (i) the period-end financial reporting process and the classification of various accounts in our consolidated financial statements, **including the presentation and disclosure of items in the consolidated statements of cash flows,** (ii) timely identification and accounting for non-routine, unusual, or complex transactions, including controls over the preparation and review of accounting memoranda addressing these matters, ~~and~~ (iii) revenue recognition, including non-routine complex revenue transactions that may also include the leasing of products, the recording of revenue transactions in the appropriate period, ~~and~~ (iv) the completeness and accuracy of accounts payable and accrued liabilities, **and (v) completeness, accuracy, valuation, and classification of each equivalent and marketable securities.** Additionally, we are in the process of designing and implementing controls related to the preparation and review of journal entries and account reconciliations to ensure proper segregation of duties. We are in the process of designing and maintaining formal accounting policies, procedures, and controls to achieve complete, accurate, and timely financial accounting, reporting, and disclosures, ~~including controls over the preparation and review of account reconciliations and journal entries.~~ We are in the process of designing and implementing information technology general controls, including controls over program change management, the review and update of user access rights and privileges, controls over batch jobs and data backups, and program development approvals and testing. In April 2022, we went live on a new Enterprise Resource Planning ("ERP") system and have implemented, and continue to implement, IT general controls related to the new system. While we are undertaking efforts to remediate these material weaknesses, the material weaknesses will not be considered remediated until our remediation plan has been fully implemented, the applicable controls operate for a sufficient period of time, and we have concluded, through testing, that the newly implemented and enhanced controls are operating effectively. **As disclosed in Part II, Item 9A – Controls and Procedures, of this Annual Report on Form 10-K, our management has concluded that our internal control over financial reporting was not effective as of December 31, 2023, and our independent registered public accounting firm rendered an adverse**

opinion on our internal control over financial reporting, as a result of the material weaknesses described above. At this time, we cannot predict the success of **our remediation efforts or the outcome of our assessment of** such efforts or the ~~outcome of our assessment of the remediation~~ efforts. We can give no assurance that our efforts will remediate these material weaknesses in our internal control over financial reporting, or that additional material weaknesses will not be identified in the future. The effectiveness of our internal control over financial reporting is subject to various inherent limitations, including cost limitations, judgments used in decision making, assumptions about the likelihood of future events, the possibility of human error and the risk of fraud. If we are unable to remediate the material weaknesses, our ability to record, process, and report financial information accurately, and to prepare the consolidated financial statements within the time periods specified by the rules and regulations of the SEC, could **continue to** be adversely affected which, in turn, may adversely affect our reputation and business and the trading price of our common stock. As a public company, we are required, pursuant to Section 404 (a) of the Sarbanes-Oxley Act, to furnish a report by management on the effectiveness of our internal control over financial reporting for each Annual Report on Form 10-K filed with the SEC. This assessment includes disclosure of any material weaknesses identified by our management in internal control over financial reporting. Once we cease to be an emerging growth company, our independent registered public accounting firm will also be required, pursuant to Section 404 (a) of the Sarbanes-Oxley Act, to attest to the effectiveness of our internal control over financial reporting in each annual report on Form 10-K to be filed with the SEC. We are also required to disclose material changes made in our internal control over financial reporting on a quarterly basis. Failure to comply with the Sarbanes-Oxley Act could potentially subject us to sanctions or investigations by the SEC, the stock exchange on which our securities are listed or other regulatory authorities, which would require additional financial and management resources. Compliance with Section 404 requires that we incur substantial costs and expend significant management efforts. Any failure to implement new or improved controls, or difficulties encountered in their implementation, could result in errors in our consolidated financial statements that could result in a restatement of our financial statements and could cause us to fail to meet our reporting obligations, any of which could diminish investor confidence in us and cause a decline in the price of our common stock. In addition, any such failures could result in litigation or regulatory actions by the SEC or other regulatory authorities, **which could further result in** loss of investor confidence, **a decline in the price of our common stock,** delisting of our securities and, harm to our reputation and financial condition, and / or diversion of financial and management resources from the operation of our business. Failure to comply with applicable anti-corruption legislation, export controls, economic sanctions and other governmental laws and regulations could result in fines, and criminal penalties and materially adversely affect our business, financial condition, and results of operations. We are required to comply with anti-corruption and anti-bribery laws in the jurisdictions in which we operate, including the Foreign Corrupt Practices Act, or FCPA, in the United States, the UK Bribery Act, or the Bribery Act, and other similar laws in other countries in which we do business. As a result of doing business in foreign countries, including through reseller partners and agents, we will be exposed to a risk of violating anti-corruption laws. Some of the international locations in which we will operate have developing legal systems and may have higher levels of corruption than more developed nations. The FCPA prohibits us or any third party acting on our behalf from **corruptly** promising, authorizing, making, offering, or providing anything of value to foreign officials for the purposes of obtaining or retaining business or securing any improper business advantage. We may deal with both governments and state-owned business enterprises, the employees of which are considered foreign officials for purposes of the FCPA. The FCPA further requires us to keep and maintain books and records that accurately reflect transactions and dispositions of assets and to maintain a system of internal accounting controls. The Bribery Act also prohibits “commercial” bribery not involving foreign officials, facilitation payments, and the receipt of bribes, while providing a defense to a charge of failure to prevent bribery to companies that demonstrate they had in place adequate procedures to prevent bribery. We **may deal with both governments and state-owned business enterprises, the employees of which are considered foreign officials for purposes of the FCPA. Some of the international locations in which we will operate have developing legal systems and may have higher levels of corruption than more developed nations. As a result of doing business in foreign countries, including through reseller partners and agents, we will be exposed to a risk of violating anti-corruption laws.** We are also required to comply with applicable export controls and economic and trade sanctions laws and regulations, such as those administered and enforced by OFAC, the U. S. Department of State, and the U. S. Department of Commerce. Our global operations expose us to the risk of violating, or being accused of violating these laws. Although we have adopted policies and procedures reasonably designed to promote compliance with such laws, there can be no assurance that such policies or procedures will work effectively at all times or protect us against liability under these or other laws for actions taken by our employees, reseller partners, and other third parties who are acting on our behalf with respect to our business. If we are not in compliance with anti-corruption laws and other laws governing the conduct of business with government entities and / or officials (including local laws) or export controls and economic and trade ~~sanctions~~ **sanction** laws and regulations, we may be subject to criminal and civil penalties and other remedial measures, which could harm our business, financial condition, results of operations, cash flows, and prospects. In addition, investigations of any actual or alleged violations of such laws or policies related to us could harm our business, financial condition, results of operations, cash flows, and prospects. ~~The long-term impacts of the COVID-19 pandemic, or other similar public health developments, could have an adverse effect on business, results of operations, and financial condition. We face various risks and uncertainties related to the uncertain, ongoing impact of COVID-19, and the possibility of other public health developments, which has led to disruption and volatility in the global economy and capital markets, increasing the cost of capital and adversely impacting access to capital. It has, and may continue to, disrupt third-party contract manufacturers and supply chain. We may also experience customer payment delays for our products which could negatively impact our results of operations. We may also experience some delays in installation of our products at customers' facilities, which could lead to postponed revenue recognition for those transactions. The long-term effects of COVID-19 on the global economy and on us are difficult to assess or predict and may include a further decline in the market prices of our~~

products, risks to employee health and safety, risks for the deployment of our products and services and reduced sales in geographic locations impacted. Any of these factors may have a material and adverse effect on our business operations and results of operations.

Risks Related to Our Common Stock and Warrants The market price of our common stock and warrants is likely **has been highly and may continue** to be highly volatile, and you may lose some or all of your investment. The trading price of our common stock as well as warrants **has been** is likely to be highly volatile **since their initial listing on the NASDAQ** and may **continue** be subject to **fluctuate wide-widely** fluctuations in response to a variety of factors, including the following: • **actual or anticipated fluctuations in our financial condition and results of operations;** • **the financial projections we may provide to the public, any changes in these projections or our failure to meet these projections;** • **failure of securities analysts to initiate or maintain coverage of our company, changes in financial estimates or ratings by any securities analysts who follow our company, or our failure to meet these estimates or the expectations of investors;** • **changes in financial markets or macroeconomic conditions, including, for example, due to the effects of recession or slow economic growth in the United States and abroad, high inflation and interest rates, bank failures, fuel prices, international currency fluctuations, corruption, political instability, acts of war, including the conflicts in Europe and the Middle East, and acts of terrorism;** • **changes in market valuations of similar companies;** • **the impact of a pandemic (such as COVID-19 or variants thereof), pandemic epidemic or a similar future outbreak of disease or similar public health concern on our business;** • **changes in financial markets or macroeconomic conditions, including, for example, due to the effects of recession or slow economic growth in the United States and abroad, rising inflation and interest rates, fuel prices, international currency fluctuations, corruption, political instability, acts of war, including the conflict involving Russia and Ukraine, and acts of terrorism;** • **the inability to maintain the listing of our shares of common stock on the NASDAQ;** • **the inability to recognize the anticipated benefits of the Merger, which may be affected by, among other things, competition in our industry, our ability to grow and manage growth profitability, and retain our key employees;** • **lawsuits threatened or filed against us;** • **anticipated or actual changes in laws, or regulations or government policies applicable laws to or our regulations business;** • **increases in compliance or enforcement inquiries and government inquiries or investigations (such as the ongoing SEC and FTC matters);** • **risks relating to the uncertainty of our projected financial information; and** • **risks related to the organic and inorganic growth of our business and the timing of expected business milestones;** • **short sales, hedging, and other derivative transactions involving our common stock; and** • **the other factors described in this "Risk Factors" section of this Annual Report on Form 10-K. Furthermore, short sellers or those that directly or indirectly assist short sellers may attempt to engage in manipulative activity intended to drive down the market price of a target company's stock. We believe we have in the past been the subject of negative public attacks by certain non-governmental entities purporting to be objective media outlets, and while we reviewed the allegations published in their associated reports and believe them to be unsubstantiated and false, we may in the future become subject to similar attacks, which may lead to increased volatility in the price of our common stock.** In addition, the stock markets—market have **has** experienced extreme price and volume fluctuations that have affected and continue to affect the market prices of equity securities of many companies. These fluctuations have often been unrelated or disproportionate to the operating performance of those companies. **Volatility in our share price could subject us to securities class action litigation. In the past, securities class action litigation has often been brought against a company following a decline in the market price of its securities or the completion of a merger. We may be the target of this type of litigation in the future. Securities litigation against us could result in substantial costs and a diversion of management's attention and resources, which could harm our business, financial condition, and results of operations.** Certain of our warrants are accounted for as liabilities and the changes in value of such warrants could have a material effect on our financial results. On April 12, 2021, the Acting Director of the Division of Corporation Finance and Acting Chief Accountant of the SEC together issued a statement regarding the accounting and reporting considerations for warrants issued by special purpose acquisition companies entitled "Staff Statement on Accounting and Reporting Considerations for Warrants Issued by Special Purpose Acquisition Companies ("SPACs")" (the "SEC Statement"). Specifically, the SEC Statement focused on certain settlement terms and provisions related to certain tender offers following a business combination, which terms are similar to those contained in the warrant agreement governing our public warrants. We evaluated the accounting treatment of our public warrants and determined to classify such warrants as derivative liabilities measured at fair value, with changes in fair value each period reported in earnings. Due to the recurring fair value measurement, we **expect that we will** recognize non-cash gains or losses on our public warrants each reporting period. **The and that the** amount of such gains or losses could be material. **Our The Company's** accounting treatment of the public warrants is based on our current interpretation of the SEC Statement and other **related** guidance and may change in light of any further interpretive **guidance or new** guidance, as may be applicable. Certain of our earn-out shares and founder shares are accounted for as liabilities and the changes in value of such shares could have a material effect on our financial results. We evaluated the accounting treatment of **(i) our earn-out shares and founder (ii) 4,312,500 shares of NHIC Class B common stock owned by certain NHIC shareholders which were converted into shares of the Company's stock in connection with the Merger, (the "Founder Shares")** and determined to classify such shares as liabilities measured at fair value, with changes in fair value each period reported in earnings. Due to the recurring fair value measurement, we **expect that we will** recognize non-cash gains or losses on our earn-out and founder shares each reporting period. **The and that the** amount of such gains or losses could be material. **Volatility in our share price could subject us to securities class action litigation. In the past, securities class action litigation has often been brought against a company following a decline in the market price of its securities or the completion of a merger. If we face such litigation, it could result in substantial costs and a diversion of management's attention and resources, which could harm our business.** Because we do not **anticipate paying intend to pay** any cash dividends **in for** the foreseeable future, capital appreciation, if any, would be your sole source of gain. We currently **intend to anticipate that we will** retain **any** future earnings for the development, operation and expansion of our business and **we do not anticipate intend to**

declaring **declare** or paying **pay** any cash dividends for the foreseeable future. As a result, capital appreciation, if any, of our common stock would be your sole source of gain on an investment in such shares for the foreseeable future. Future sales, **or the perception of future sales**, of common stock **by our existing security holders in the public market** may cause the market price of our securities to drop significantly **decline**. Future sales of a substantial number of our common stock into the **public market**, even if **particularly sales by our directors and executive officers** ~~our~~ **or by holders** business is doing well. Certain of our stockholders that hold Founder Shares were in, **or the perception** past subject to lock-up restrictions that have expired **these sales might occur, could cause the market price of our common stock to decline**. The shares held by our directors and executive officers, as well as the Founder Shares that vested at the closing of the Merger may be freely resold in the public market, except that any shares held by our affiliates, as defined in Rule 144 under the Securities Act would only be able to be sold in compliance with Rule 144. Certain of the Founder Shares are also subject to certain share-performance-based vesting provisions whereas ~~where~~ **where 50-25 %** of the Founder Shares **will** vested at the closing of the Merger, 25 % of the Founder Shares shall vest on or before **July 16, 2026** the fifth anniversary of the Closing if the closing share price of the common stock equals or exceeds \$ 12. 50 over any 20 trading days within a 30- day trading period and the remaining 25 % will vest on or before **July 16, 2026** the fifth anniversary of the Closing if the closing share price of the common stock equals or exceeds \$ 15. 00 over any 20 trading days within any 30- day trading period. ~~Now~~ **In addition, as of December 31, 2023, we had stock options, restricted stock units (" RSUs "), and performance stock units (" PSUs") outstanding that, if fully exercised or vested, would result in these-- the issuance of 33** lock-up restrictions have expired, **751, 207** such stockholders are not restricted from selling shares of our common stock held by, **All of them-- the shares** that were previously subject to the lock-up restrictions, other than by applicable securities laws. Sales of our common stock as issuable upon the exercise of stock options, and the shares reserved for future issuance under our plans, are registered for public resale under the Securities Act. Accordingly, these shares can be freely sold in the public market upon issuance subject to applicable vesting requirements, compliance with Rule 144, and other restrictions ~~end~~ **provided under the terms of the applicable plan and /** vesting conditions are satisfied may make it more difficult for ~~or us~~ to sell equity securities in the future at a time **award agreements entered into with participants and any such** at a price that we deem appropriate. These sales could also cause **adversely affect** the trading market price of our common stock. **We are unable to predict the timing** fall and make it more difficult for ~~or us~~ to sell shares **effect of such sales on the market price** of our common stock. We are **no longer** an "emerging growth company," **" or a " smaller reporting company"** and we cannot be certain if the reduced reporting requirements applicable to emerging growth companies **and smaller reporting companies** will **no longer apply** make our shares less attractive to investors ~~us~~. We are **As of December 31, 2023, we lost our status as an " emerging growth company ;"** as defined in the Jumpstart Our Business Startups Act of 2012 (the **" JOBS Act "**) and a **" smaller reporting company "**). For as **defined under the Exchange Act. As a result, we are no long longer entitled** as we continue to **rely on** be an emerging growth company, we may take advantage of exemptions from various reporting **certain disclosure and compliance** requirements that are applicable to other public companies that are not "emerging growth companies," including exemption from compliance with, **but not limited to:** • the auditor attestation requirements- **requirement of to have our independent registered public accounting firm audit our internal controls over financial reporting under** Section 404 (b) of the Sarbanes- Oxley Act ; • of 2002, reduced disclosure obligations regarding executive compensation and exemptions from the requirements- **requirement that we adopt new or revised accounting standards when they are applicable to public companies, instead of holding delaying their adoption until they are applicable to private companies; and • the requirement that we hold a non- nonbinding--- binding** advisory vote on executive compensation and **obtain** stockholder approval of any golden parachute payments not previously approved. **Additionally, although we are permitted to continue to provide scaled disclosures permitted for a smaller reporting company through our Annual Report on Form 10- K for the fiscal year ended December 31, 2023, beginning with our first quarterly report on Form 10- Q for the quarter ending March 31, 2024, we will no longer be permitted to rely on exemptions from those requirements that are applicable to smaller reporting companies, including, but not limited to, the requirement that we provide full and more detailed disclosures regarding executive compensation. We will remain an expect that the loss of emerging growth company status until the earlier of (1) the last day of the fiscal year (a) following the fifth anniversary of the completion of the initial public offering, (b) in which we have total annual gross revenue of at least \$ 1. 235 billion or (c) in which we are deemed to be a large accelerated filer or (2) the date on which we have issued more than \$ 1. 0 billion in non-convertible debt during the prior three- year period. In addition, under the JOBS Act, emerging growth companies can delay adopting new or revised accounting standards until such time as those standards apply to private companies. We have elected to use this extended transition period for complying with new or revised accounting standards and, therefore, we will not be subject to the same new or revised accounting standards as other public companies that are not emerging growth companies. Even after we no longer qualify as an **and** emerging growth company, we may still qualify as a " smaller reporting company **status and**," which would allow us to take advantage of many of the same exemptions from disclosure requirements including exemption from compliance with the **these additional** auditor attestation requirements **may place a burden on our financial and management resources and increase our accounting, legal, and financial compliance costs associated with corporate governance requirements applicable to us as a public company, including under the rules and regulations of the SEC, Section 404 (b) of the Sarbanes- Oxley Act, the Dodd- Frank Wall Street Reform and Customer Protection Act of 2002- 2010 , the Securities Act, and reduced disclosure obligations regarding executive compensation in the Exchange Act, as well as the Nasdaq rules, and make some activities more time consuming. We also expect these rules and regulations to make it more difficult and more expensive for us to obtain director and officer liability insurance, and we may be required to incur substantial costs to maintain the same our- or similar coverage periodic reports and proxy statements. We cannot predict or estimate the amount or timing of additional costs we may incur to respond to these requirements. The impact****

of these requirements could also make it more difficult for us to attract and retain qualified individuals to serve on our board of directors, our board committees or as executive officers. Furthermore, if our additional disclosures in future SEC filings are perceived as insufficient or inadequate by investors will find our or regulatory authorities, common stock less attractive because it may rely on these -- the exemptions. If some investors find our common stock less attractive as a result, there may be a less active trading market for our common stock and our market price may of our stock could decline and we could be more volatile subject to actions by stockholders or regulatory authorities. General Risk Factors Increasing attention to, and evolving expectations for, environmental, social, and governance (“ ESG ”) initiatives could increase our costs, harm our reputation, or otherwise adversely impact our business. Companies across industries are facing increasing scrutiny from a variety of stakeholders related to their ESG practices. Expectations regarding voluntary ESG initiatives and disclosures may result in increased costs (including but not limited to increased costs related to compliance, stakeholder engagement, contracting, and insurance), changes in demand for certain offerings, enhanced compliance or disclosure obligations, or other adverse impacts to our business, financial condition, or results of operations. While we may at times engage in voluntary initiatives (such as voluntary disclosures, certifications, or goals, among others) to improve the ESG profile of our company and / or offerings or to respond to stakeholder demands, such initiatives may be costly and may not have the desired effect. Expectations around companies’ management of ESG matters continues- continue to evolve rapidly, in many instances due to factors that are out of our control. We may experience pressure to make commitments relating to ESG matters that affect us; however, we may not agree that particular initiatives will be appropriate for our business, and we may not be able to implement such initiatives because of potential costs or technical or operational obstacles, which may adversely impact our reputation or stakeholder relations. If we do not, or are perceived by stakeholders to not, take sufficient action to respond to ESG matters, we may be subject to investor or regulator engagement on our ESG initiatives and disclosures, even if such initiatives are currently voluntary. Certain market participants, including major institutional investors and capital providers, use third- party benchmarks and scores to assess companies’ ESG profiles in making investment or voting decisions. Unfavorable ESG ratings could lead to increased negative investor sentiment towards us, which could negatively impact our share price as well as our access to and cost of capital. To the extent ESG matters negatively impact our reputation, it may also impede our ability to compete as effectively to attract and retain employees or customers, which may adversely impact our operations. In addition, we expect there will likely be increasing levels of regulation, disclosure- related and otherwise, with respect to ESG matters. For example, the SEC has proposed requirements to disclose a variety of climate- related information, in addition to other rules, which could require us to incur significant costs for monitoring and compliance. This and other regulations will likely lead to increased costs as well as scrutiny that could heighten all of the risks identified in this risk factor. Additionally, many of our customers and suppliers may be subject to similar expectations, which may augment or create additional risks, including risks that may not be known to us. If we cannot maintain our company culture as it we grows- grow, we could lose the innovation, teamwork, passion, and focus on execution that we believe contributes to our success and our business may be harmed. We believe that a critical component to our success has been our mission- driven company culture based on our shared commitment to make the world a safer place to live, work, learn, and play, which we believe fosters innovation, teamwork, passion for customers and focus on execution, and facilitates critical knowledge transfer, knowledge sharing, and professional growth. We have invested substantial time and resources in building our team within this company culture. Any failure to preserve our culture could negatively affect our ability to retain and recruit personnel and to effectively focus on and pursue our corporate objectives. As we grow and develop our public company infrastructure and processes, we may find it difficult to maintain these important aspects of our company culture. If we fail to maintain our company culture, our business may be adversely impacted. Our reported financial results may be adversely affected by changes in accounting principles generally accepted in the United States. U. S. generally- Generally accepted- Accepted accounting- Accounting principles- Principles (" GAAP ") are subject to interpretation by the Financial Accounting Standards Board (FASB), the SEC, and various bodies formed to promulgate and interpret appropriate accounting principles. A change in these principles or interpretations could have a significant effect on our reported results of operations and could affect the reporting of transactions already completed before the announcement of such change. If securities or industry analysts do not publish research or reports about us, or publish negative reports, our stock price and trading volume could decline. The trading market for our common stock will depend, in part, on the research and reports that securities or industry analysts publish about us. We do not have any control over these analysts reports. If our financial performance fails to meet analyst estimates or one or more of the analysts who cover us downgrade our common stock, change their opinion, or reduce their target stock price on us, our stock price would likely decline. If one or more of these analysts cease coverage of us our company or fail to regularly publish reports on about us, we could lose visibility in the financial markets, which could cause our stock price or trading volume to decline.