Risk Factors Comparison 2025-03-31 to 2024-04-01 Form: 10-K

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

Investing in our common stock involves a high degree of risk. You should consider carefully the risks and uncertainties described below, together with all of the other information in this report, including our consolidated financial statements and related notes, before deciding whether to purchase shares of our common stock. If any of the following risks is realized, our business, operating results, financial condition and prospects could be materially and adversely affected. In that event, the price of our common stock could decline, and you could lose part or all of your investment. Moreover, the risks described below are not the only ones that we face. Additional risks not presently known to us or that we currently deem immaterial may also affect our business, operating results, prospects or financial condition. You should carefully consider these risk factors, together with all of the other information included in this Annual Report on Form 10- K as well as our other publicly available filings with the SEC. Risks Related to Our Growth If our business does not grow as we expect, or if we fail to manage our growth effectively, our operating results and business prospects would suffer. Our ability to successfully grow our business depends on a number of factors including our ability to: • accelerate our acquisition of new customers; • further sell expansions of coverage areas to our existing customers; • expand our international footprint; • expand into new vertical markets, such as precision policing, and security solutions; • increase awareness of the benefits that our solutions offer; • maintain our competitive and technology leadership position; and • manage our business successfully through macroeconomic pressures, such as **the imposition of tariffs,** inflation, rising interest rates, and past and potential future disruptions in access to bank deposits and lending commitments due to bank failures, and any resulting impact on economic conditions, including conditions impacting the availability of funding for our public safety ~~solution~~ **solutions** . As usage of our solutions grows, we will need to continue to make investments to develop and implement new or updated solutions, technologies, security features and cloud- based infrastructure operations. In addition, we will need to appropriately scale our internal business systems and our services organization, including the suppliers of our detection equipment and customer support services, to serve our growing customer base. Any failure of, or delay in, these efforts could impair the performance of our solutions and reduce customer satisfaction. Further, our growth could increase quickly and place a strain on our managerial, operational, financial and other resources, and our future operating results depend to a large extent on our ability to successfully manage our anticipated expansion and growth. To manage our growth successfully, we will need to continue to invest in sales and marketing, research and development, and general and administrative functions and other areas. We are likely to recognize the costs associated with these investments earlier than receiving some of the anticipated benefits, and the return on these investments may be lower, or may develop more slowly, than we expect, which could adversely affect our operating results. If we are unable to manage our growth effectively, we may not be able to take advantage of market opportunities or develop new solutions or upgrades to our existing solutions, satisfy customer requirements, maintain the quality and security of our solutions or execute on our business plan, any of which could have a material adverse effect on our business, operating results and financial condition. Our quarterly results of operations may fluctuate significantly due to a wide range of factors, which makes our future results difficult to predict. Our revenues and results of operations could vary significantly from quarter to quarter as a result of various factors, many of which are outside of our control, including: • the expansion or contraction of our customer base; • the renewal or non- renewal of subscription agreements with, and expansion of coverage areas by, existing customers; **or cross- selling of other products or services to existing customers;** • the size, timing, terms and deployment schedules of our sales to both existing and new customers; • the introduction of products or services that may compete with us for the limited funds available to our customers, and changes in the cost of such products or services; • changes in our customers' and potential customers' budgets; • our ability to control costs, including our operating expenses; • our ability to hire, train and maintain our direct sales force; • the timing of satisfying revenues recognition criteria in connection with initial deployment and renewals; • fluctuations in our effective tax rate; • the concentration of our revenue in a small number of large contracts with the potential for fluctuations and delays; and • general economic factors, such as **the imposition of tariffs,** inflation, rising interest rates, past and potential future disruptions in access to bank deposits and lending commitments due to bank failures, and political conditions, both domestically and internationally. For example, with regard to the concentration of our revenue, for the year ended December 31, ~~2023~~ **2024** , the City of New York and the City of Chicago ~~,~~ **as** our two largest customers accounted for ~~25~~ **23** % and ~~9~~ **10** % of the Company' s total revenues, respectively. **Our** ~~We have extended our~~ contract with the City of Chicago ~~through~~ **ended in** November 2024 ~~,~~ ~~but~~ **and we renewed our two contracts with** ~~there~~ -- **the** ~~is no guarantee we will receive another extension~~ **City of New York in the first quarter of 2025** . ~~Additionally, we are experiencing a~~ **The ending of our contract with the City of Chicago and any inability to renew or** ~~delay~~ **delays** in ~~our ShotSpotter~~ renewal **of our contract** with ~~Puerto Rico, see~~ the **City** ~~risk entitled " Our success depends on maintaining and increasing our sales, which depends on factors we cannot control, including the availability~~ of **New York** ~~funding to our customers. " Any delays in renewal of our contracts~~ or any of the other factors above or other factors discussed elsewhere in this report ~~may~~ **will** result in fluctuations in our revenues and operating results, meaning that quarter- to- quarter comparisons of our revenues, results of operations and cash flows may not necessarily be indicative of our future performance. Because of the fluctuations described above, our ability to forecast revenues is limited and we may not be able to accurately predict our future revenues or results of operations. In addition, we base our current and future expense levels on our operating plans and sales forecasts, and our operating expenses are expected to increase in the short term. Accordingly, we may not be able to reduce our costs sufficiently to compensate for an unexpected shortfall in revenues, and even a small shortfall in revenues could disproportionately and adversely affect our financial results for that quarter. The

variability and unpredictability of these and other factors could result in our failing to meet or exceed financial expectations for a given period. Because we generally recognize our subscription revenues ratably over the term of our contract with a customer, fluctuations in sales will not be fully reflected in our operating results until future periods. Our revenues are primarily generated from subscriptions to our solutions. With the exception of a small number of legacy customers, our customers do not have the right to take possession of our equipment or software platform. Revenues from subscriptions to our software platform are recognized ratably over the subscription period beginning on the date that the subscription is made available to the customer, which we refer to as the " go- live " date. Our agreements with our customers typically range from one to three years. As a result, much of the revenues that we report in each quarter are attributable to agreements entered into during previous quarters. Consequently, a decline in sales, customer renewals or market acceptance of our solutions in any one quarter would not necessarily be fully reflected in the revenues in that quarter and would negatively affect our revenues and profitability in future quarters. This ratable revenue recognition also makes it difficult for us to rapidly increase our revenues through additional sales in any period, as revenues from new customers generally are recognized over the applicable agreement term. Our subscription- based approach may result in uneven recognition of revenues. We recognize subscription revenues over the term of a subscription agreement. Once we enter into a ShotSpotter contract with a customer, there is a delay until we begin recognizing revenues while we survey the coverage areas, obtain any required consents for installation, and install our sensors, which together can take up to several months or more. We begin recognizing revenues from a ShotSpotter sale only when all of these steps are complete and the solution is live. While most of our customers elect to renew their subscription agreements following the expiration of a term, in some cases, they may not be able to obtain the proper approvals or funding to complete the renewal prior to such expiration. For these customers, we stop recognizing subscription revenues at the end of the current term, even though we may continue to provide services for a period of time while the renewal process is completed. Once the renewal is complete, we then recognize subscription revenues for the period between the expiration of the term of the agreement and the completion of the renewal process. The variation in the timeline for deploying our solutions and completing renewals may result in fluctuations in our revenues, which could cause our results to differ from projections. Additionally, while we generally invoice for 50 % of the contract cost upon a customer' s go- live date, our cash flows may be volatile and will not match our ~~revenues~~ **revenue** recognition. We have not been profitable in the past and may not achieve or maintain profitability in the future. We had a net loss of $ **9.** 2 ~~.7~~ million for the year ended December 31, ~~2023~~ **2024** and as of December 31, ~~2023~~ **2024**, we had an accumulated deficit of $ ~~95~~ **104** . ~~1~~ **3** million. Although we posted net income in ~~2019,~~ 2020 and 2022, we had a net loss in 2021 and **2023** ~~we had net losses prior to 2019~~ . We are not certain whether we will be able to maintain enough revenues from sales of our solutions to sustain or increase our growth or maintain profitability in the future. We also expect our costs to increase in future periods, which could negatively affect our future operating results if our revenues do not increase. In particular, we expect to continue to expend substantial financial and other resources on: • higher costs to procure the sensors required for our solutions due to inflationary pressures; • sales and marketing, including a significant expansion of our sales organization, both domestically and internationally; • research and development related to our solutions, including investments in our engineering and technical teams; • acquisition of complementary technologies or businesses, such as our acquisition of **LEEDS** ~~HunchLab technology in October 2018~~ , ~~our acquisition of~~ **LLC, now known as** Technologic **,** in November 2020, our acquisition of Forensic Logic in January 2022 and our acquisition of SafePointe in August 2023; • continued international expansion of our business; and • general and administrative expenses. These investments may not result in increased revenues or growth in our business. If we are unable to increase our revenues at a rate sufficient to offset the expected increase in our costs, our business, operating results and financial position may be harmed, and we may not be able to maintain profitability over the long term. Rising inflation rates have resulted in decreased demand for our products and services and have increased our operating costs. 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 maintain profitability in the future. We may require additional capital to fund our business and support our growth, and our inability to generate and obtain such capital on acceptable terms, or at all, could harm our business, operating results, financial condition and prospects. We intend to continue to make substantial investments to fund our business and support our growth. In addition, we may require additional funds to respond to business challenges, including the need to develop new features or enhance our solutions, improve our operating infrastructure or acquire or develop complementary businesses and technologies. As a result, in addition to the revenues we generate from our business and our existing cash balances, we may need to engage in additional equity or debt financings to provide the funds required for these and other business endeavors. 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 such additional financing on terms favorable to us, if at all. If we are unable to obtain adequate financing or financing on terms satisfactory to us 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. In addition, our inability to generate or obtain the financial resources needed may require us to delay, scale back, or eliminate some or all of our operations, which may have a material adverse effect on our business, operating results, financial condition and prospects. Risks Related to Our Public Safety Business **Our success depends on maintaining and increasing our sales, which depends on factors we cannot control, including the availability of funding to our customers.** To date, substantially all of our revenues have been derived from contracts with local governments and their agencies, in particular the police departments of major cities in the United States. To a lesser extent, we also generate revenues from federal

agencies, foreign governments and higher education institutions. We believe that the success and growth of our business will continue to depend on our ability to add new police departments and other government agencies, domestically and internationally, as customers of our public safety ~~solution~~ **solutions** and new universities, corporate campuses and key infrastructure and transportation centers as customers of our security solutions. Many of our target customers have restricted budgets, such that we are forced to compete with programs or solutions that offer an alternative use of the same funds. A number of factors could cause current and / or potential customers to delay or refrain from purchasing our solutions, prevent expansion of, or reduce coverage areas and / or terminate use of our solutions, including: • decreases or changes in available funding, including **as a result of policies implemented by Trump administration' s Department of Government Efficiency within the Office of Management and Budget (" DOGE "),** tax revenues, budgetary allocations, government grants and other government funding programs; • potential delays or changes in appropriations or other funding authorization processes; • changes in fiscal or contracting policies; • macro- and / or local economic changes, such as **the imposition of tariffs,** inflation, rising interest rates, and past and potential future disruptions in access to bank deposits and lending commitments due to bank failures, that may affect customer funding; • changes in elected or appointed officials; • changes in public perception of the accuracy of our solutions and the appropriate use of our solutions by law enforcement, including as a result of negative publicity; and • changes in laws or public sentiment regarding privacy or surveillance. For example, our ~~existing~~ contract with the City of Chicago ~~remains~~ **ended** in ~~effect until~~ November 2024 and we ~~may~~ **were** not ~~be~~ able to renew or extend our contract ~~on reasonable terms, if at all~~. The City of Chicago ~~is~~ **was** one of our largest customers and represented ~~9 % and~~ 10 % of our total revenues for the year ended December 31, ~~2023 and 2022, respectively. Additionally, while we signed an interim contract with Puerto Rico through January 31,~~ 2024 ~~, we are working on the delayed renewal with Puerto Rico, which represented 1. 6 % and 2. 6 % of our total revenues for the year ended December 31, 2023 and 2022, respectively. If we are unable to renew our contracts with the City of Chicago or Puerto Rico, this could have a material adverse effect on our operating results~~. The past and potential future disruptions in access to bank deposits and lending commitments due to bank failures, geopolitical developments such as the conflicts between Ukraine and Russia **and** in ~~Israel~~ **the Middle East**, and other macroeconomic pressures in the United States and the global economy such as **the imposition of tariffs,** rising inflation and interest rates, supply chain constraints, labor market shortages, energy prices and recession fears, and any associated impact on economic conditions, could also cause or exacerbate any of the foregoing. The occurrence of any of the foregoing would impede or delay our ability to maintain or increase the amount of revenues derived from these customers, which could have a material adverse effect on our business, operating results and financial condition. Contracting with government entities can be complex, expensive, and time- consuming. The procurement process for government entities is in many ways more challenging than contracting in the private sector. We must comply with laws and regulations relating to the formation, administration, performance and pricing of contracts with government entities, including U. S. federal, state and local governmental bodies. These laws and regulations may impose added costs on our business or prolong or complicate our sales efforts, and failure to comply with these laws and regulations or other applicable requirements could lead to claims for damages from our customers, penalties, termination of contracts and other adverse consequences. Any such damages, penalties, disruptions or limitations in our ability to do business with government entities could have a material adverse effect on our business, operating results and financial condition. Government entities often require highly specialized contract terms that may differ from our standard arrangements. For example, if the federal government provides grants to certain state and local governments for our solutions, and such governments do not continue to receive these grants, then these customers have the ability to terminate their contracts with us without penalty. Government entities often impose compliance requirements that are complicated, require preferential pricing or " most favored nation " terms and conditions, or are otherwise time- consuming and expensive to satisfy. Compliance with these special standards or satisfaction of such requirements could complicate our efforts to obtain business or increase the cost of doing so. **Due to the nature of our business as a software- as- a- service provider, we are occasionally unable to meet certain requirements related to the utilization of small businesses in providing our services.** Even if we do meet these special standards or requirements, the increased costs associated with providing our solutions to government customers could harm our margins. Additionally, even once we have secured a government contract, the renewal process can be lengthy and as time- consuming as the initial sale, and we may be providing our service for months past the contract expiration date without certainty if the renewal agreement will be signed or not. During periods of economic uncertainty resulting from the past and potential future disruptions in access to bank deposits and lending commitments due to bank failures, geopolitical developments such as the conflicts between Ukraine and Russia and in ~~Israel~~ **the Middle East**, and other macroeconomic pressures in the United States and the global economy such as **the imposition of tariffs,** rising inflation and interest rates, supply chain constraints, labor market shortages, energy prices and recession fears, and any associated impact on economic conditions, these risks are more pronounced than usual, as government entities struggle with reduced levels of resources related to implications of such global events. Changes in the underlying regulatory conditions, political landscape or required procurement procedures that affect these types of customers could be introduced prior to the completion of our sales cycle, making it more difficult or costly to finalize a contract with a new customer or expand or renew an existing customer relationship. For example, customers may require a competitive bidding process with extended response deadlines, review or appeal periods, or customer attention may be diverted to other government matters, postponing the consideration of the purchase of our products. Such delays could harm our ability to provide our solutions efficiently and to grow or maintain our customer base. If we are unable to further penetrate the public safety market, our revenues may not grow. Our ability to increase revenues will depend in large part on our ability to sell our current and future public safety solutions. For example, our ability to have our ShotSpotter customers renew their annual subscriptions and expand their mileage coverage or purchase and implement our other products, such as CaseBuilder ~~(formerly ShotSpotter Investigate)~~ and ResourceRouter ~~(formerly ShotSpotter Connect)~~, drives our ability to increase our revenues. Most of our ShotSpotter customers begin using our solution in a limited coverage area. Our experience has been, and we expect will

continue to be, that after the initial implementation of our solutions, our new customers typically renew their annual subscriptions, and many also choose to expand their coverage area. However, some customers may choose to not renew or reduce their coverage **, including as a negative reaction to price increases** . If existing customers do not choose to renew or expand their coverage areas, or choose to reduce their coverage, our revenues will not grow as we anticipate, or may even decline. During periods of economic uncertainty resulting from past and potential future disruptions in access to bank deposits and lending commitments due to bank failures, geopolitical developments such as the conflicts between Ukraine and Russia and in ~~Israel~~ **the Middle East** , and other macroeconomic pressures in the United States and the global economy, such as **the imposition of tariffs,** rising inflation and interest rates, supply chain constraints, labor market shortages, energy prices and recession fears, and any associated impact on economic conditions, this risk is more pronounced than usual, as our customers' priorities may change or they may have greater uncertainty regarding the availability of funding for our solutions as a result. Our ability to further penetrate the market for our public safety solutions depends on several factors, including: maintaining a high level of customer satisfaction and a strong reputation among law enforcement; increasing the awareness of our SoundThinking solutions and their benefits; the effectiveness of our marketing programs; the availability of funding to our customers; geopolitical developments and other macroeconomic pressures as described above; our ability to expand our solutions; and the costs of our solutions. Some potential public safety customers may be reluctant or unwilling to use our solution for a number of reasons, including concerns about additional costs **or increased prices** , unwillingness to expose or lack of concern regarding the extent of gun violence in their community, uncertainty regarding the reliability and security of cloud- based offerings or lack of awareness of the benefits of our public safety solutions. If we are unsuccessful in expanding the coverage of SoundThinking solutions by existing public safety customers or adding new customers, our revenues and growth prospects would suffer. Our sales cycle can be lengthy, time- consuming and costly, and our inability to successfully complete sales could harm our business. Our sales process involves educating prospective customers and existing customers about the use, technical capabilities and benefits of our solutions. Prospective customers, especially government agencies, often undertake a prolonged evaluation process that may last up to nine months or more and that typically involves comparing the benefits of our solutions to alternative uses of funds. We may spend substantial time, effort and money on our sales and marketing efforts without any assurance that our efforts will produce any sales. In addition, in 2011 the Federal Bureau of Investigation' s (the " FBI ") Criminal Justice Information Services Division (the " CJIS ") issued the CJIS Security Policy, a set of standards for organizations that access criminal justice information (" CJI "). CJIS developed this policy to better protect the data it delivers to federal, state and local law enforcement agencies, from services like the National Crime Information Center, the Integrated Automated Fingerprint Identification System and the National Incident Based Reporting System. The policy is also designed to protect CJI that comes from sources other than the FBI. As part of the process of implementing CaseBuilder for a customer, we ~~will~~ **may** have ~~to complete a rigorous application process~~ to become an approved CJIS compliant vendor. ~~While this~~ **In some states** CJIS ~~compliant~~ **compliance** ~~vendor approval process~~ is **required** ~~based upon the FBI' s CJIS Security Policy~~ , a separate process will have to be completed in **locations** ~~each state~~ where CaseBuilder will be implemented. We are continually improving our security, compliance, and processes. Our general processes are based on the NIST- 800- 53 standard with some aspects also being controlled by CJIS. In the fourth quarter of ~~2022~~ **2024** , an audit of our processes under a SOC2 Type 2 audit was completed. These initiatives require fiscal and time investments. Failure to obtain a SOC2 Type 2 audit report or to be compliant with the CJIS standard **or HIPAA** could adversely affect our reputation and sales, as well as the availability of our solutions in certain markets. Additionally, events affecting our customers' budgets or missions may occur during the sales cycle that could negatively impact the size or timing of a purchase after we have invested substantial time, effort and resources into a potential sale, contributing to more unpredictability in the growth of our business. If we are unable to succeed in closing sales with new and existing customers, our business, operating results and financial condition will be harmed. During periods of economic uncertainty resulting from the past and potential future disruptions in access to bank capital and lending commitments due to bank failures, geopolitical developments such as the conflicts between Ukraine and Russia and in ~~Israel~~ **the Middle East** , and other macroeconomic pressures in the United States and the global economy, such as **the imposition of tariffs,** rising inflation and interest rates, supply chain constraints, labor market shortages, energy prices and recession fears, and any associated impact on economic conditions, this risk is more pronounced than usual, as our customers' priorities may change or they may have greater uncertainty regarding the availability of funding for our solutions as a result. Changes in the availability of federal funding to support local law enforcement efforts could impact our business. Many of our customers rely to some extent on funds from the U. S. federal government in order to purchase and pay for our solutions. Any reduction in federal funding for local law enforcement efforts could result in our customers having less access to funds required to continue, renew, expand or pay for our solutions. Social unrest, protests against racial inequality, protests against police brutality and movements such as " Defund the Police " have increased in past years. **In addition, four members of Congress previously requested the Inspector General of the Department of Homeland Security to investigate the appropriateness of the use of federal funds to purchase our ShotSpotter solution. Furthermore, the New York Comptroller previously issued a report with certain conclusions questioning the accuracy and value of our ShotSpotter solution, which that we disputed in a formal reply on the basis that they were misinformed and did not give adequate weight to the New York Police Department' s views. Additionally, funds under the American Rescue Plan Act (" ARPA "), which is a federal stimulus bill that included emergency funding for state, local, territorial and tribal governments to aid public health and economic recovery from the COVID- 19 pandemic, are nearing their limit. Changes in the availability of federal funding, such as under ARPA or due to policies implemented by DOGE, may lead to changes in the operations of federal agencies, which may adversely impact our business and operating results.** These events may directly or indirectly affect municipal and police agency budgets, including federal funding available to current and potential customers. If federal funding is reduced or eliminated and our customers cannot find alternative sources of funding to purchase our solutions, our business will be harmed. ~~Federal~~

~~stimulus funding or earnings as a result of the COVID- 19 pandemic had been provided; however, we do not know whether additional stimulus funding will be made available to our existing or potential customers, and many state and local governments anticipate budget shortfalls without additional funding. Further, the allocation and prioritization of stimulus funds or earnings is uncertain and may change. There is no guarantee that additional funding will be made available to fund our solutions.~~ Real or perceived false positive gunshot alerts or false positive security threat detection, or failure or perceived failure to generate alerts for actual gunfire **or missed weapon detection** could adversely affect our customers and their operations, damage our brand and reputation and adversely affect our growth prospects and results of operations. A false positive alert, in which a non- gunfire incident is reported as gunfire or detection of items that do not actually represent security threats, could result in an unnecessary rapid deployment of police officers and first responders, which may raise unnecessary fear among the occupants of a community or facility, and may be deemed a waste of police and first responder resources. A failure to alert law enforcement or security personnel of actual gunfire or security threats (false negative) **or missed weapon detection** could result in a less rapid or no response by police officers and first responders, increasing the probability of injury or loss of life. Both false positive alerts and the failure to generate alerts of actual gunfire or security threats (false negative) **or missed weapon detection** may result in customer dissatisfaction, potential loss of confidence in our solutions, and potential liabilities to customers or other third parties, any of which could harm our reputation and adversely impact our business and operating results. Additionally, third parties may misunderstand or misrepresent what constitutes a false positive or false negative and generate negative publicity regarding our solutions. For example, a ~~May~~ **June** ~~2021~~ **2024** report by the ~~MacArthur Center for Justice~~ **New York City Comptroller** appears to argue that any incident that does not result in a police report is a false positive. The perception of a false positive alert or of a failure to generate an alert **or missed weapon detection** , even where our customers understand that our solutions were utilized correctly, could lead to negative publicity or harm the public perception of our solutions, which could harm our reputation and adversely impact our business and operating results. The nature of our business may result in undesirable press coverage or other negative publicity, which could adversely affect our growth prospects and results of operations. Our solutions are used to assist law enforcement and first responders in the event that gunfire is detected. Even when our solutions work as intended, the incidents detected by our solutions could lead to injury, loss of life and other negative outcomes, and such events are likely to receive negative publicity. If we fail to detect an incident, or if we detect an incident, such as a terrorist attack or active- shooter event, but the response time of law enforcement or first responders is not sufficiently quick to prevent injury, loss of life, property damage or other adverse outcomes, we may receive negative media attention. At times, our data or information concerning our techniques and processes may become a matter of public record due to legal or other obligations (for example, as a result of public- records requests or subpoenas to provide information or to testify in court), and we may receive negative media attention as a result. Our reputation and our business may be harmed by inaccurate reporting, which could have an adverse impact on new sales or renewals or expansions of coverage areas by existing customers, which would adversely impact our financial results and future prospects. For example, in July 2021, VICE Media, LLC (“ VICE ”) falsely accused us of illegal behavior, which has had a material adverse effect on our business. We initiated a defamation lawsuit against VICE that has since been dismissed. The role of our solutions and our personnel in criminal prosecutions or other court proceedings may result in unfavorable judicial rulings that generate negative publicity or otherwise adversely impact new sales or renewals or expansions of coverage areas by existing customers, which would adversely impact our financial results and future prospects. For instance, a court ruling limiting or excluding evidence related to information gathered through our systems or to the operation of our systems in a judicial proceeding could harm public perceptions of our business and solutions. Economic uncertainties or downturns, or political changes, could limit the availability of funds available to our existing and potential customers, which could materially and adversely affect our business. Economic uncertainties or downturns could adversely affect our business and operating results. Negative conditions in the general economy both in the United States and abroad, including past and potential future disruptions in access to bank deposits and lending commitments due to bank failures, conditions resulting from changes in gross domestic product growth, labor market shortages, **the imposition of tariffs,** inflation, interest rates, financial and credit market fluctuations, political deadlock, natural catastrophes, warfare, geopolitical tensions, such as the ongoing conflicts between Russia and Ukraine and in ~~Israel~~ **the Middle East** , terrorist attacks, climate change and global pandemics, could cause a decrease in funds available to our existing and potential customers and negatively affect the rate of growth of our business **. Changes in the availability of federal funding, such as under ARPA, and the leadership of federal agencies under the Trump administration, including return- to- office policy, hiring freeze, layoffs, and other policies implemented by DOGE, may lead to changes in the operations of federal agencies, which may adversely impact our business and operating results** . These economic conditions may make it extremely difficult for our customers and us to forecast and plan future budgetary decisions or business activities accurately, and they could cause our customers to reevaluate their decisions to purchase our solutions, which could delay and lengthen our sales cycles or result in cancellations of planned purchases. Furthermore, during challenging economic times or as a result of political changes, our customers may tighten their budgets and face constraints in gaining timely access to sufficient funding or other credit, which could result in an impairment of their ability to make timely payments to us. In turn, we may be required to increase our allowance for doubtful accounts, which would adversely affect our financial results. We cannot predict the timing, strength or duration of any economic slowdown, instability or recovery, generally or within any particular industry, or the impact of political changes. If the economic conditions of the general economy or industries in which we operate worsen from present levels, or if past political changes result in less funding being available to purchase our solutions, our business, operating results, financial condition and cash flows could be adversely affected. New competitors may enter the market for our public safety ~~solution~~ **solutions** . If cities and other government entities increase their efforts to reduce gun violence or our solutions gain visibility in the market, companies could decide to enter into the public safety ~~solution~~ **solutions** market and thereby increase the competition we face. In addition to other gunshot detection products **, vehicle and plate identification and weapons detection** , we also compete with other

technologies and solutions targeting our public safety customers' resources for law enforcement **, security teams** and crime prevention. Our competitors could benefit from the disclosure of our data or information concerning our techniques and processes due to legal or other obligations (for example, as a result of public- records requests or subpoenas to provide information or to testify in court). Because there are several possible uses for these limited budgetary resources, if we are not able to compete successfully for these limited resources, our business may not grow as we expect, which could adversely impact our revenues and operating results. Concerns regarding privacy and government- sponsored surveillance may deter customers from purchasing our solutions. Governmental agencies and private citizens have become increasingly sensitive to real or perceived government or third- party surveillance and may wrongly believe that our outdoor sensors allow customers to listen to private conversations and monitor private citizen activity. Our sensors are not designed for " live listening " and are triggered only by loud impulsive sounds that may likely be gunfire. However, perceived privacy concerns may result in negative media coverage and efforts by private citizens to persuade municipalities, educational institutions or other potential customers not to purchase our precision policing solutions for their communities, campuses or facilities. In addition, laws may exist or be enacted to address such concerns that could impact our ability to deploy our solutions. For example, the City of Toronto, Canada decided against using SoundThinking solutions because the Ministry of the Attorney General of Ontario indicated that it may compromise Section 8 of Canada' s Charter of Rights and Freedoms, which relates to unreasonable search and seizure. If customers choose not to purchase our solutions due to privacy or surveillance concerns, then the market for our solutions may develop more slowly than we expect, or it may not achieve the growth potential we expect, any of which would adversely affect our business and financial results. Ongoing social unrest may have a material adverse effect on our business, the future magnitude or duration of which we cannot predict with accuracy. We may be adversely affected by ongoing social unrest, protests against racial inequality, protests against police brutality and movements such as " Defund the Police " or increases in such unrest that may occur in the future, and such unrest may be exacerbated by inaccurate information or negative publicity regarding our solutions. These events may directly or indirectly affect police agency budgets and funding available to current and potential customers. Participants in these events may also attempt to create the perception that our solutions are contributing to the " problem " which may adversely affect us, our business and results of operations, including our revenues, earnings and cash flows from operations. Strategic and Operational Risks If we are unable to sell our solutions into new markets, **or cross-sell our other solutions to our existing customers,** our revenues may not grow. Part of our growth strategy depends on our ability to increase sales of our security and public safety solutions in markets outside of the United States **. and to increase sales of our other solutions to our existing ShotSpotter customers** . We are focused on expanding the sales of these solutions into new markets, but customers in these new markets may not be receptive or sales may be delayed beyond our expectations, causing our revenue growth and growth prospects to suffer. **We are also trying to increase our cross- selling efforts targeted at our existing customers, for example by encouraging our existing ShotSpotter customers to implement our other solutions such as CaseBuilder and ResourceRouter but there is no assurance that our existing customers will be receptive to our other solutions.** During periods of economic uncertainty resulting from the past and potential future disruptions in access to bank deposits and lending commitments due to bank failures, geopolitical developments such as the conflicts between Ukraine and Russia and in ~~Israel~~ **the Middle East** , and other macroeconomic pressures in the United States and the global economy such as **the imposition of tariffs,** rising inflation and interest rates, supply chain constraints, labor market shortages, energy prices and recession fears, and any associated impact on economic conditions, this risk is more pronounced than usual. Our ability to successfully face these challenges depends on several factors, including increasing the awareness of our solutions and their benefits; the effectiveness of our marketing programs; the costs of our solutions; our ability to attract, retain and effectively train sales and marketing personnel; and our ability to develop relationships with communication carriers and other partners. If we are unsuccessful in developing and marketing our solutions into new markets, **or growing our revenues from our existing customers through cross- selling,** new markets for our solutions might not develop or might develop more slowly than we expect, ~~either~~ **or we may not be able to expand our relationships with our existing customers, all** of which would harm our revenues and growth prospects. The failure of our solutions to meet our customers' expectations or of our solutions generally could, in some cases, result in injury or loss of life, and could harm our reputation, which may have a material adverse effect on our business, operating results and financial condition. Promoting and demonstrating the utility of our solutions as useful, reliable and important tools for law enforcement and security personnel is critical to the success of our business. Our ability to secure customer renewals, expand existing customer coverage areas, and enter into new customer contracts is dependent on our reputation and our ability to deliver our solutions effectively. We believe that our reputation among police departments using SoundThinking solutions is particularly important to our success. Our ability to meet customer expectations will depend on a wide range of factors, including: • our ability to continue to offer high- quality, innovative and accurate precision policing solutions; • our ability to maintain continuous gunshot detection monitoring during high outdoor-noise activity periods such as New Year' s Day, the Fourth of July and Cinco de Mayo, and Carnival for international deployments; • our ability to maintain high customer satisfaction, including meeting our service level agreements standards; • the perceived value and quality of our solutions; • differences in opinion regarding the metrics that measure the success of our solutions; • our ability to successfully communicate the unique value proposition of our solutions; • our ability to provide high-quality customer support; • any misuse or perceived misuse of our solutions; • interruptions, delays or attacks on our platform; • litigation- or regulation- related developments; and • damage to or degradation of our sensors or sensor network **and cameras** by third parties. In some cases, if our solutions 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, subject us to litigation and potential claims against us, and have an adverse effect on our business, operating results and financial condition. There is no guarantee that our solutions 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. If our products fail to detect security threats for any reason, including failures due to customer personnel or security processes, it may also 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. Interruptions or performance problems associated with our technology and infrastructure may adversely affect our business and results of operations. We have in the past experienced, and may in the future experience, performance issues due to a variety of factors, including infrastructure changes, human or software errors, intentional or accidental damage to our technology (including sensors **and cameras**), website or third- party hosting disruptions or capacity constraints due to a number of potential causes including technical failures, natural disasters or security attacks. If our security is compromised, our platform is unavailable or our users are unable to receive our alerts or otherwise communicate with our IRC reviewers, within a reasonable amount of time or at all, our business could be negatively affected. In some instances, we may not be able to identify the cause or causes of these performance problems within an acceptable period of time. In addition, our IRC department personnel operate either ~~remotely~~ **in a hybrid work model** or out of our offices. Any interruption or delay in service from our IRC, such as from a communications or power outage, could limit our ability to deliver our solutions. In addition, it may become increasingly difficult to maintain and improve the performance of our solutions, especially during peak usage times as the capacity of our IRC operations reaches its limits. If there is an interruption or delay in service from our IRC operations and a gunshot is detected but not reviewed in the allotted time, our software will flag the incident for off- line review. This may result in delayed notifications to our customers and as a result, we could experience a decline in customer satisfaction with our solutions and our reputation and growth prospects could be harmed. We expect to continue to make significant investments to maintain and improve the performance of our solutions. To the extent that we do not effectively address capacity constraints, upgrade our systems as needed and continually develop our technology to accommodate actual and anticipated changes in technology, our business, operating results and financial condition may be adversely affected. We rely on wireless carriers to provide access to wireless networks through which our acoustic sensors communicate with our cloud- based backend and with which we provide our notification services to customers, and any interruption of such access would impair our business. We rely on wireless carriers, mainly AT & T and Verizon, to provide access to wireless networks for machine- to- machine data transmissions, which are an integral part of our services. Our wireless carriers may suspend wireless service to expand, maintain or improve their networks. These wireless carriers perform routine maintenance and periodic software and firmware updates that may damage our sensors or make them inoperable. Any suspension or other interruption of services would adversely affect our ability to provide our services to our customers and may adversely affect our reputation. In addition, the terms of our agreements with these wireless carriers provide that either party can cancel or terminate the agreement for convenience. If one of our wireless carriers were to terminate its agreement with us, we would need to source a different wireless carrier and / or modify our equipment during the notice period in order to minimize disruption in the performance of our solutions. Price increases or termination by our wireless carriers or changes to existing contract terms could have a material adverse effect on our business, operating results and financial condition. Furthermore, our reliance on wireless carriers may require updates to our technology and making such updates could also result in interruptions in our service or increase our costs of operations. We may not be able to successfully implement new technologies or adapt existing technologies to changing market demands. If we are unable to adapt timely to changing technologies, market conditions or customer preferences, our business, operating results and financial condition could be materially and adversely affected. Natural disasters, infectious disease outbreaks, power outages or other events impacting us or our customers could harm our operating results and financial condition. We recognize revenue on a subscription basis as our solutions are provided to our customers over time. If our services are disrupted due to natural disasters, infectious disease outbreaks, power outages or other events that we cannot control, we may not be able to continue providing our solutions as expected. When we stop providing coverage, we also stop recognizing revenues as a result of the affected subscription agreement. If we are forced to discontinue our services due to natural disasters, power outages and other events outside of our control, our revenues may decline, which would negatively impact our results of operations and financial condition. In addition, we may face liability for damages caused by our sensors in the event of heavy weather, hurricanes or other natural disasters. We may also incur additional costs to repair or replace installed sensor networks damaged by heavy weather, hurricanes or other natural disasters. Any of our facilities or operations may be harmed or rendered inoperable by natural or man- made disasters, including earthquakes, tornadoes, hurricanes, wildfires, floods, nuclear disasters, acts of terrorism or other criminal activities, global pandemics, and power outages, which may render it difficult or impossible for us to operate our business for some period of time or decrease productivity. For example, our primary IRC and a data center that hosts some of our customer services are located in the San Francisco Bay Area, a region known for seismic activity. Our facilities would likely be costly to repair or replace, and any such efforts would likely require substantial time. In addition, like many companies, at the beginning of the COVID- 19 pandemic, we implemented a work from home policy. We expect to work in a hybrid work model for the foreseeable future. This policy may negatively impact productivity of our employees. Any disruptions in our operations could negatively impact our business and operating results and harm our reputation. In addition, we may not carry business insurance or may not carry sufficient business insurance to compensate for losses that may occur. Any such losses or damages could have a material adverse effect on our business, operating results and financial condition. In addition, the facilities of significant vendors, including the manufacturer of our proprietary acoustic sensor, may be harmed or rendered inoperable by such natural or man- made disasters, which may cause disruptions, difficulties or material adverse effects on our business. The incurrence of debt may impact our financial position and subject us to additional financial and operating restrictions. On September 27, 2018, we entered into a senior secured revolving credit facility with Umpqua Bank (the " Umpqua Credit Agreement ") and in November 2022, we amended the Umpqua Credit Agreement to, among other things, extend the maturity date from November 27, 2022 to October 15, 2024, increase the revolving credit commitment from $ 20. 0 million to $ 25. 0 million and increase the letter of credit sub- facility from $ 6. 0 million to $ 7. 5 million. In February 2024, we

amended the Umpqua Credit Agreement to extend the maturity date from October 15, 2024 to October 15, 2025. As of December 31, ~~2023~~ **2024**, there was $ ~~7~~ **4**. 0 million outstanding on our line of credit. Under the Umpqua Credit Agreement, we are subject to various negative covenants that limit, subject to certain exclusions, our ability to incur indebtedness, make loans, invest in or secure the obligations of other parties, pay or declare dividends, make distributions with respect to our securities, redeem outstanding shares of our stock, create subsidiaries, materially change the nature of our business, enter into related party transactions, engage in mergers and business combinations, the acquisition or transfer of our assets outside of the ordinary course of business, grant liens or enter into collateral relationships involving company assets or reincorporate, reorganize or dissolve the company. These covenants could adversely affect our financial health and business and future operations by, among other things: • making it more difficult to satisfy our obligations, including under the terms of the Umpqua Credit Agreement; • limiting our ability to refinance our debt on terms acceptable to us or at all; • limiting our flexibility to plan for and adjust to changing business and market conditions and increasing our vulnerability; • limiting our ability to use our available cash flow to fund future acquisitions, working capital, business activities, and other general corporate requirements; and • limiting our ability to obtain additional financing for working capital to fund growth or for general corporate purposes, even when necessary to maintain adequate liquidity. We are also required to maintain certain financial covenants tied to our leverage, interest charges and profitability. Our ability to meet such covenants (those negative covenants discussed in the preceding paragraph) or other restrictions can be affected by events beyond our control, and our failure to comply with the financial and other covenants would be an event of default under the Umpqua Credit Agreement. If an event of default under the Umpqua Credit Agreement, has occurred and is continuing, the outstanding borrowings thereunder could become immediately due and payable, and we would then be required to cash collateralize any letters of credit then outstanding, and the lender could refuse to permit additional borrowings under the facility. We have in the past obtained waivers for the financial covenant tied to our profitability, the acquisition and investment covenants related to our acquisition of SafePointe and name change covenant for failure to provide notice of our corporate name change and of the name change of LEEDS, LLC to Technologic Solutions, LLC. We cannot assure you that we would have sufficient assets to repay those borrowings and, if we are unable to repay those amounts, the lender could proceed against the collateral granted to them to secure such indebtedness. We have pledged substantially all of our assets as collateral, and an event of default would likely have a material adverse effect on our business. The competitive landscape for our security solutions is evolving. The market for security solutions for university campuses, corporate campuses and transportation and key infrastructure centers includes a number of available options, such as video surveillance and increased human security presence. Because there are several possible uses of funds for security needs, we may face increased challenges in demonstrating or distinguishing the benefits of ShotSpotter for ~~Highways, ShotSpotter for~~ Campus and ShotSpotter for Corporate. In particular, while we have seen growing interest in our security solutions, interest in the indoor gunshot detection offering was limited, and as a result, in June 2018, we made the strategic decision to cease indoor coverage as part of our service offering. If we experience declining interest in any of our offerings, we may cease offering such impacted solution in the future. Failure to effectively develop and expand our sales and marketing capabilities could harm our ability to increase our customer base and achieve broader market acceptance of our solutions. To increase total customers and customer coverage areas and to achieve broader market acceptance of our solutions, we will need to expand our sales and marketing organization and increase our business development resources, including the vertical and geographic distribution of our sales force and our teams of account executives focused on new accounts and responsible for renewal and growth of existing accounts. Our business requires that our sales personnel have particular expertise and experience in working with law enforcement agencies, other government organizations and higher education institutions. We may not achieve revenue growth from expanding our sales force if we are unable to hire, develop and retain talented sales personnel with appropriate experience, if our new sales personnel are unable to achieve desired productivity levels in a reasonable period of time or if our sales and marketing programs are not effective ~~. During the COVID- 19 pandemic, this risk was more pronounced than usual, as our sales and marketing organization were unable to travel and meetings with current and potential customers were more difficult to conduct~~ . Our strategy includes pursuing acquisitions, and our inability to successfully integrate newly acquired technologies, assets or businesses, or our becoming subject to certain liabilities assumed or incurred with our acquisitions, may harm our financial results. Future acquisitions of technologies, assets or businesses, which are paid for partially or entirely through the issuance of stock or stock rights, could dilute the ownership of our existing stockholders. We acquired Technologic in November 2020, Forensic Logic in January 2022 and SafePointe and intellectual property assets in August 2023 in order to enhance our SafetySmart platform. We will continue to evaluate and consider potential strategic transactions, including acquisitions of, or investments in, businesses, technologies, services, products and other assets in the future. We also may enter into relationships with other businesses to expand our platform and applications, which could involve preferred or exclusive licenses, additional channels of distribution, discount pricing or investments in other companies. We believe that part of our continued growth will be driven by acquisitions of other companies or their technologies, assets, businesses and teams. Acquisitions in the future that we complete will give rise to risks, including: • incurring higher than anticipated capital expenditures and operating expenses; • failing to assimilate the operations and personnel or failing to retain the key personnel of the acquired company or business; • failing to integrate the acquired technologies, or incurring significant expense to integrate acquired technologies, into our platform and applications; • disrupting our ongoing business; • diverting our management' s attention and other company resources; • failing to maintain uniform standards, controls and policies; • incurring significant accounting charges; • impairing relationships with our customers and employees; • finding that the acquired technology, asset or business does not further our business strategy, that we overpaid for the technology, asset or business or that we may be required to write off acquired assets or investments partially or entirely; • failing to realize the expected synergies of the transaction; • being exposed to unforeseen liabilities and contingencies that were not identified prior to acquiring the company; and • being unable to generate sufficient revenues and profits from acquisitions to offset the associated acquisition costs. Fully integrating an

acquired technology, asset or business into our operations may take a significant amount of time. We may not be successful in overcoming these risks or any other problems encountered with the acquisition of and integration of Technologic, Forensic Logic and SafePointe, intellectual property assets acquired or any future acquisitions. To the extent that we do not successfully avoid or overcome the risks or problems related to any such acquisitions, our results of operations and financial condition could be harmed. Acquisitions also could impact our financial position and capital requirements or could cause fluctuations in our quarterly and annual results of operations. Acquisitions could include significant goodwill and intangible assets, which may result in future impairment charges that would reduce our stated earnings. We may incur significant costs in our efforts to engage in strategic transactions and these expenditures may not result in successful acquisitions. Additionally, there may be liabilities that we fail to discover while conducting due diligence for acquisitions, that we inadequately assess or that are not properly disclosed to us. In particular, to the extent that any acquired company failed to comply with or otherwise violated applicable laws or regulations, failed to fulfill contractual obligations to counterparties or incurred material liabilities or obligations to other parties that are not identified during the diligence process, we, as the successor owner, may be financially responsible for these violations, failures and liabilities and may suffer financial or reputational harm or otherwise be adversely affected. We also may be subject to litigation or other claims in connection with an acquired company. Any material liabilities we incur that are associated with our acquisitions could harm our business, operating results and financial condition. We expect that the consideration we might pay for any future acquisitions of technologies, assets, businesses or teams could include stock, rights to purchase stock, cash or some combination of the foregoing. If we issue stock or rights to purchase stock in connection with future acquisitions, net income per share and then- existing holders of our common stock may experience dilution. The nature of our business exposes us to inherent liability risks. Our gunshot detection solutions are designed to communicate real-time alerts of gunfire incidents to police officers and first responders. Similarly, our weapons detection solution obtained from our SafePointe acquisition is designed to identify potential threats and alert security personnel. Due to the nature of such applications, we are potentially exposed to greater risks of liability for employee acts or omissions or system failures than may be inherent in other businesses. Although substantially all of our customer agreements contain provisions limiting our liability to our customers, we cannot be certain that these limitations will be enforced or that the costs of any litigation related to actual or alleged omissions or failures would not have a material adverse effect on us even if we prevail. Further, certain of our insurance policies and the laws of some states may limit or prohibit insurance coverage for punitive or certain other types of damages or liability arising from gross negligence, or other issues, such as damages caused due to installation of our sensors on buildings owned by third parties, and we cannot assure you that we are adequately insured against the risks that we face. Real or perceived errors, failures, ~~vulnerabilities,~~ or bugs in our software could adversely affect our operating results and growth prospects. Because our software is complex, undetected errors, failures or bugs may occur. Our software is often installed and used with different operating systems, system management software, ~~and~~ equipment and networking configurations, which may cause errors or failures of our software or other aspects of the computing environment into which it is deployed. In addition, deployment of our software into computing environments may expose undetected errors, compatibility issues, failures or bugs in our software. Despite our testing, errors, failures ~~, vulnerabilities~~ , or bugs may not be found in our software until it is released to our customers. Moreover, our customers could incorrectly implement or inadvertently misuse our software, which could result in customer dissatisfaction and adversely impact the perceived utility of our products as well as our brand. Any of these real or perceived errors, compatibility issues, failures or bugs in our software could result in negative publicity, reputational harm, loss of or delay in market acceptance of our software, loss of competitive position or claims by customers for losses sustained by them. In any such event, we may be required, or may choose, for customer relations or other reasons, to expend additional resources in order to correct the problem. Alleviating any of these problems could require significant expenditures of our capital and other resources and could cause interruptions or delays in the use of our solutions, which could cause us to lose existing or potential customers and could adversely affect our operating results and growth prospects. ~~Any interruptions or delays in service from our third- party providers could impair our ability to make our solutions available to our customers, resulting in customer dissatisfaction, damage to our reputation, loss of customers, limited growth and reduction in revenue. We currently use third-party data center hosting facilities to host certain components of our solutions. Our operations depend, in part, on our third-party providers' abilities to protect these facilities against damage or interruption from natural disasters, power or communications failures, cyber incidents, criminal acts and similar events. In the event that any of our third- party facility arrangements is terminated, or if there is a lapse of service or damage to a facility, we could experience service interruptions in our solutions as well as delays and additional expenses in arranging new facilities and services. People continuing to work remotely may increase the likelihood of service interruptions or cyber incidents at these data center hosting facilities. Any changes in third- party service levels at our data centers or any errors, defects, disruptions, cyber incidents or other performance problems with our solutions could harm our reputation. Any damage to, or failure of, the systems of the communications providers with whom our data center provider contracts could result in interruptions to our solutions. The occurrence of spikes in usage volume, natural disasters, cyber incidents, acts of terrorism, vandalism or sabotage, closure of a facility without adequate notice or other unanticipated problems could result in lengthy interruptions in the availability of our services. Problems faced by these network providers, or with the systems by which they allocate capacity among their customers, including us, could adversely affect the experience of our customers. People continuing to work remotely may increase the likelihood of these problems with such network providers and their capacity allocation systems. Interruptions in our services might cause us to issue refunds to customers and subject us to potential liability. Further, our insurance policies may not adequately compensate us for any losses that we may incur in the event of damage or interruption, and therefore the occurrence of any of the foregoing could subject us to liability, cause us to issue credits to customers or cause customers not to renew their subscriptions for our applications, any of which could materially and adversely affect our business.~~ If our information technology systems or data, or those of third parties ~~upon which~~ **with whom** we ~~rely~~ **work** , are or were compromised ~~, our solutions may be perceived as not~~

~~being secure~~ , our customers may be harmed and we could experience adverse consequences **resulting from such compromise** , including **,** but not limited to **,** regulatory investigations or actions; litigation or mass arbitration demands; fines and penalties; disruptions of our business operations; reputation harm; loss of revenue or profits; loss of customers or sales; and other adverse consequences. Our operations **and those of the third parties with whom we work,** involve the **processing,** collection, receipt, storage, storage processing, generation, use, transfer, disclosure, protection, disposal of, transmission, and sharing (collectively, " processing ") of proprietary, confidential ~~,~~ and sensitive data, including personal information, intellectual property, trade secrets and other sensitive information such as gunfire incident data, including date, time, address and GPS coordinates, occurring in our customer' s coverage area (collectively, " sensitive information "). Additionally, our systems **process** ~~read, write, store and transfer~~ information from third parties including criminal justice information. Cyber- attacks, malicious internet-based activity, online and offline fraud, and other similar activities threaten the confidentiality, integrity, and availability of our sensitive information and information technology systems, and those of the third parties ~~upon which~~ **with whom** we ~~rely~~ **work** . Such threats are prevalent and continue to increase generally, and are increasingly difficult to detect, and come from a variety of sources, including traditional computer " hackers, " threat actors, " hacktivists, " organized criminal threat actors, personnel (such as through theft or misuse), sophisticated nation states, and nation- state- supported actors. Some actors now engage and are expected to continue to engage in cyber- attacks, including without limitation nation- state actors for geopolitical reasons and in conjunction with military conflicts and defense activities. During times of war and other major conflicts, we, the third parties ~~upon which~~ **with whom** we ~~rely~~ **work** , and our customers may be vulnerable to a heightened risk of these attacks, including retaliatory cyber- attacks, that could materially disrupt our systems and operations, supply chain, and ability to produce, sell and distribute our ~~goods~~ **products** and services. We and the third parties upon which we rely may be subject to a variety of evolving threats, including but not limited to social- engineering attacks (including through deep fakes, which may be increasingly more difficult to identify as fake, phishing attacks), malicious code (such as viruses and worms), malware (including as a result of advanced persistent threat intrusions), denial- of- service attacks, credential stuffing, credential harvesting, personnel misconduct or error, and supply- chain attacks, software bugs, server malfunctions, software or hardware failures, loss of data or other information technology assets, attacks enhanced or facilitated by ~~artificial intelligence (" AI ")~~ , telecommunications failures, earthquakes, fires, floods, and other similar threats. For example, in November 2023, we discovered that a ~~recently~~ terminated employee logged on to an employee resource, obtained our confidential information, and began posting some of the information publicly on social media. We took steps to remove the information and prevent the former employee from posting the information again, but we are uncertain to what extent this will reoccur and ~~the postings~~ **if it does, whether it** will ~~affect~~ **materially impact** our business or operations. In particular, ransomware attacks are becoming increasingly prevalent and severe and can lead to significant interruptions in our operations, ability to provide our products or services, loss of data and income, reputational harm, and diversion of funds. Extortion payments may alleviate the negative impact of a ransomware attack, but we may be unwilling or unable to make such payments due to, for example, applicable laws or regulations prohibiting such payments. **In particular, ransomware attacks are becoming increasingly prevalent and severe and can lead to significant interruptions in our operations, ability to provide our products or services, loss of data and income, reputational harm, and diversion of funds. Extortion payments may alleviate the negative impact of a ransomware attack, but we may be unwilling or unable to make such payments due to, for example, applicable laws or regulations prohibiting such payments.** Remote work ~~has become more common and~~ has increased risks to our information technology systems and data, as more of our employees utilize network connections, computers and devices outside our premises or network, including working at home, while in transit and in public locations. ~~We~~ **It** may be ~~unable~~ **difficult and / or costly** to ~~anticipate~~ **detect, investigate, mitigate, contain, and remediate a security incident. Our efforts to do so may not be successful. Actions taken by us or the third parties with whom we work to detect, investigate, mitigate, contain, and remediate a security incident could result in outages, data losses, and disruptions of** ~~or~~ **our** ~~prevent techniques used to obtain unauthorized~~ **business. Threat actors may also gain** access ~~or~~ to ~~sabotage~~ **other networks and** systems ~~because such techniques change frequently and often are not detected until~~ after **a compromise of our networks** ~~an~~ **and systems** ~~incident has occurred~~ . As we increase our customer base and our brand becomes more widely known and recognized, third parties may increasingly seek to compromise our security controls or gain unauthorized access to customer data or other sensitive information. Further, because of the nature of the services that we provide to our customers, we may be a unique target for attacks. Future or past business transactions (such as acquisitions or integrations, including of Forensic Logic, LLC and SafePointe, LLC) expose us to additional cybersecurity risks and vulnerabilities, as we and our systems are negatively affected by vulnerabilities and weaker security controls present in acquired or integrated entities' systems, products, processes and technologies. Furthermore, we may not have adequate visibility into security issues of such acquired or integrated entities, may discover security issues that were not found during due diligence of such entities, and it may be difficult to integrate companies and their products into our information technology environment and security program. We rely on third **parties** ~~- party service providers and technologies~~ to operate critical business systems to process sensitive information in a variety of contexts, including, without limitation, cloud- based infrastructure, data center facilities, encryption and authentication technology, employee email, content delivery to customers, and other functions. We also rely on third **parties** ~~- party service providers~~ to provide other products, services, parts, or otherwise to operate our business. Our ability to monitor these third parties' information security practices is limited, and these third parties may not have adequate information security measures in place. If ~~our~~ **the** third ~~- party service providers~~ **parties with whom we work** experience a security incident or other interruption, we **have in the past and** could **in the future** experience adverse consequences. If third parties with whom we work, such as vendors or developers, violate applicable laws or our security policies, such violations may also put our systems and data at risk and could in turn have an adverse effect on our business. In addition, such a violation could expose sensitive data including; criminal justice information, and other data we are contractually obliged to keep confidential. While we may be entitled to damages if ~~our~~ **the** third ~~- party service providers~~ **parties with whom we work** fail to satisfy their

privacy or security- related obligations to us, any award may be insufficient to cover our damages, or we may be unable to recover such award **. In addition, supply- chain attacks have increased in frequency and severity, and we cannot guarantee that third parties' infrastructure in our supply chain or that of the third parties with whom we work have not been compromised** . While we have implemented security measures designed to protect against security incidents, there can be no assurance that these measures will be effective. We take steps to detect and remediate vulnerabilities **in our information systems (such as our hardware and / or software** , ~~but~~ **including that of third parties with whom** we ~~may~~ **work). We have** not ~~be able to~~ **and may not in the future, however,** detect and remediate all ~~vulnerabilities because the threats and techniques used to exploit the vulnerability change frequently and are often sophisticated in nature. Therefore,~~ such vulnerabilities **including on a timely basis. Vulnerabilities** could be exploited **and result in** ~~but may not be detected until after~~ a security incident ~~has occurred. Unremediated high risk or critical vulnerabilities pose material risks to our business~~ . Further, we may experience delays in developing and deploying remedial measures designed to address any such identified vulnerabilities. **We employ a shared responsibility model where our customers are responsible for using, configuring and otherwise implementing security measures related to our platform, services and products in a manner that meets applicable cybersecurity standards, complies with laws, and addresses their information security risk. As part of this shared responsibility security model, we make certain security features available to our customers that can be implemented at our customers' discretion, or identify security areas or measures for which our customers are responsible. For example, we recommend that customers implement Multifactor Authentication (MFA) when using our products. In certain cases where our customers choose not to implement, or incorrectly implement, those features or measures, misuse our services, or otherwise experience their own vulnerabilities, policy violations, credential exposure or security incidents, even if we are not the cause of a resulting customer security issue or incident, our customer relationships, reputation, and revenue have been and in the future may be adversely impacted.** Any of the previously identified or similar threats ~~could~~ **have in the past and may in the future** cause a security incident or other interruption that could result in unauthorized, unlawful ~~,~~ or accidental acquisition, modification, destruction, loss, alteration, encryption, disclosure of ~~,~~ or access to our sensitive information or our information technology systems, or those of the third parties upon whom we rely. A security incident or other interruption could disrupt our ability (and that of third parties upon whom we rely) to provide our solutions. We may expend significant resources or modify our business activities to try to protect against security incidents. Certain data privacy and security obligations ~~may~~ **have** ~~require~~ **required** us to implement and maintain specific security measures or industry-standard or reasonable security measures to protect our information technology systems and sensitive information. Applicable data privacy and security obligations may require us **, or we may voluntarily choose,** to notify relevant stakeholders **, including affected individuals, customers, regulators and investors,** of security incidents **, or to take other actions, such as providing credit monitoring and identity theft protection services** . Such disclosures ~~are~~ **and related actions can be** costly, and the disclosure or the failure to comply with such **applicable** requirements could lead to adverse consequences. For example, many governments have enacted laws requiring companies to notify individuals of data security incidents or unauthorized transfers involving certain types of personal information. In addition, some of our customers contractually require notification of any data security incident. If we (or a third party ~~upon~~ **with** whom we ~~rely~~ **work**) experience a security incident or are perceived to have experienced a security incident, we may experience **material** adverse consequences, such as government enforcement actions (for example, investigations, fines, penalties, audits, and inspections); additional reporting requirements and / or oversight; restrictions on processing sensitive information (including personal information); litigation (including class claims); indemnification obligations; negative publicity; reputational harm; monetary fund diversions; **diversion of management attention;** interruptions in our operations (including availability of data); financial loss; and other similar harms. Security incidents and attendant **material** consequences may prevent or cause customers to stop using our solutions, deter new customers from using our solutions, and negatively impact our ability to grow and operate our business ~~. Furthermore, security incidents experienced by our competitors, by our customers or by us may lead to public disclosures, which may lead to widespread negative publicity and significant costs. Any security compromise, whether actual or perceived, could harm our reputation, erode customer confidence in the effectiveness of our security measures, negatively impact our ability to attract new customers, cause existing customers to elect not to renew their subscriptions or subject us to third- party lawsuits, regulatory fines or other action or liability, which could materially and adversely affect our business and operating results~~ . Our contracts may not contain limitations of liability, and even where they do, there can be no assurance that limitations of liability in our contracts are sufficient to protect us from liabilities, damages, or claims related to our data privacy and security ~~incidents~~ **obligations** . While we maintain general liability insurance coverage and coverage for errors or omissions, we cannot **be** ~~assure~~ -- **sure** ~~you~~ that such coverage would be adequate or ~~would otherwise~~ **sufficient to** protect us from liabilities **arising out of** ~~or~~ **our privacy and security practices** ~~damages with respect to claims alleging compromise or loss of data~~ , ~~or~~ that such coverage will continue to be available on ~~acceptable~~ **commercially reasonable** terms or at all, or that such coverage will pay future claims. In addition to experiencing a security incident, third parties may gather, collect, or infer sensitive information about us from public sources, data brokers, or other means that reveals competitively sensitive details about our organization and could be used to undermine our competitive advantage or market position ~~. Additionally, sensitive information of the Company or our customers could be leaked, disclosed, or revealed as a result of or in connection with our employee' s, personnel' s, or vendor' s use of generative AI technologies~~ . We rely on the cooperation of customers and third parties to permit us to install our ShotSpotter sensors and SafePointe bollards on their facilities, and failure to obtain these rights could increase our costs or limit the effectiveness of our ShotSpotter and SafePointe solutions. Our ShotSpotter solution requires us to deploy ShotSpotter sensors in our customer coverage areas, which typically entails the installation of approximately 15 to 25 sensors per square mile. The ShotSpotter sensors are mounted on city facilities and third- party buildings, and occasionally on city or utility-owned light poles, and installing the sensors requires the consent of the property owners, which can be time- consuming to

obtain and can delay deployment. Generally, we do not pay a site license fee in order to install our sensors, and our contractual agreements with these facility owners provide them the right to revoke permission to use their facility with notice of generally 60 days. Our SafePointe solution requires us to install sensors, cameras, and networking equipment on our customer' s property. SafePointe does not pay a site license fee to install our sensors, cameras, and networking equipment and is typically paid by the customer to complete the installation. In almost all cases, the property is owned by the customer, and no additional approvals or consents are required. To the extent that required consents delay our ability to deploy our solutions or facility owners do not grant permission to use their facilities, revoke previously granted permissions, or require us to pay a site license fee in order to install our sensors or bollards, our business may be harmed. If we were required to pay a site license fee in order to install sensors or bollards, our deployment expenses would increase, which would impact our gross margins. If we cannot obtain a sufficient number of sensor or bollard mounting locations that are appropriately dispersed in a coverage area, the effectiveness of our ShotSpotter and SafePointe solutions would be limited, and we may need to reduce the coverage area of the solution. If we lose our ability to share a significant agency' s dataset in our CrimeTracer platform, our ability to sell that product may be adversely affected. Agencies typically share their private CJIS data sets with us through subscription agreements. If we lose access to their data sets because of a technical problem, such as a ransomware attack, or other issues that arise through no fault of our own that makes that data set inaccessible, this may result in the loss of a customer to a competitor, subscriptions not being renewed and may make it more difficult to sell CrimeTracer in that geographic region and to the federal market. If we fail to offer high- quality customer support, our business and reputation may suffer. We offer customer support 24 hours a day, seven days a week, as well as training on best practices, forensic expertise and expert witness services. Providing these services requires that our personnel have specific experience, knowledge and expertise, making it more difficult for us to hire qualified personnel and to scale up our support operations. The importance of high- quality customer support will increase as we expand our business and pursue new customers. We may be unable to respond quickly enough to accommodate short- term increases in customer demand for support services or scale our services if our business grows. Increased customer demand for these services, without corresponding revenues, could increase our costs and harm our operating results. If we do not help our customers use applications within our solutions and provide effective ongoing support, our ability to sell additional applications to, or to retain, existing customers may suffer and our reputation with existing or potential customers may be harmed. We rely on a limited number of suppliers and contract manufacturers, and our proprietary ShotSpotter sensors are manufactured by a single contract manufacturer. We rely on a limited number of suppliers and contract manufacturers. In particular, we use a single manufacturer, with which we have no long- term contract and from which we purchase on a purchase- order basis, to produce our proprietary ShotSpotter sensors. Our reliance on a sole contract manufacturer increases our risks since we do not currently have any alternative or replacement manufacturers, and we do not maintain a high volume of inventory. In the event of an interruption in our supply from our sole contract manufacturer, we may not be able to develop alternate or secondary sources without incurring material additional costs and substantial delays. Furthermore, these risks could materially and adversely affect our business if one of our contract manufacturers is impacted by a natural disaster or other interruption at a particular location because each of our contract manufacturers produces our products from a single location. Although each of our contract manufacturers has alternative manufacturing locations, transferring manufacturing to another location may result in significant delays in the availability of our sensors. Also, many standardized components used broadly in our sensors are manufactured in significant quantities in concentrated geographic regions, particularly in Greater China. As a result, protracted regional crises, or issues with manufacturing facilities could lead to eventual shortages of necessary components. It could be difficult, costly and time consuming to obtain alternative sources for these components, or to change product designs to make use of alternative components. In addition, difficulties in transitioning from an existing supplier to a new supplier could create delays in component availability that would have a significant impact on our ability to fulfill orders for our products. Many of the key components used to manufacture our proprietary ShotSpotter sensors also come from limited or sole sources of supply. In addition, the lead times associated with certain components are lengthy and preclude rapid changes in quantities and delivery schedules. Developing alternate sources of supply for these components may be time- consuming, difficult, and costly, and we or our suppliers may not be able to source these components on terms that are acceptable to us, or at all, which may undermine our ability to fill our orders in a timely manner. For example, for our ShotSpotter sensors, it may take a significant amount of time to identify a contract manufacturer that has the capability and resources to build the sensors to our specifications. Identifying suitable suppliers and contract manufacturers is an extensive process that requires us to become satisfied with their quality control, technical capabilities, responsiveness and service, financial stability, regulatory compliance, and labor and other ethical practices. Accordingly, the loss of any key supplier or contract manufacturer could adversely impact our business, operating results and financial condition. Our solutions use third- party software and services that may be difficult to replace or cause errors or failures of our solutions that could lead to a loss of customers or harm to our reputation and our operating results. We license third- party software and depend on services from various third parties for use in our solutions. In the future, such software or services may not be available to us on commercially reasonable terms, or at all. Any loss of the right to use any of the software or services could result in decreased functionality of our solutions until equivalent technology is either developed by us or, if available from another provider, is identified, obtained and integrated, which could harm our business. In addition, any errors or defects in or failures of the third- party software or services could result in errors or defects in our solutions or cause our solutions to fail, which could harm our business and be costly to correct. Many of these providers attempt to impose limitations on their liability for such errors, defects or failures, and if enforceable, we may have additional liability to our customers or third- party providers that could harm our reputation and increase our operating costs. We will need to maintain our relationships with third- party software and service providers, and obtain from such providers software and services that do not contain any errors or defects. Any failure to do so could adversely impact our ability to deliver effective products to our customers and could harm our operating results. We use artificial intelligence in our products and services which may result in

operational challenges, legal liability, reputational concerns and competitive risks. We currently use and intend to leverage generative AI processes and algorithms and our own evolving cognitive and analytical applications into our daily operations, including by deploying generative AI into our products and services, which may result in adverse effects to our financial condition, results or reputation. Generative AI products and services leverage existing and widely available technologies, such as Chat GPT- 4 and its successors, or alternative large language models or other processes. The use of generative AI processes at scale is relatively new, and may lead to challenges, concerns and risks that are significant or that we may not be able to predict, especially if our use of these technologies in our products and services becomes more important to our operations over time. Use of generative AI in our products and services may be difficult to deploy successfully due to operational issues inherent to the nature of such technologies, and our customers may not adopt or integrate our new services as intended. For example, AI algorithms use machine learning and predictive analytics which may lead to flawed, biased, and inaccurate results, which could lead to customer rejection or skepticism of such products. Emerging ethical issues surround the use of AI, and if our deployment or use of AI becomes controversial, we may be subject to reputational risk. Further, unauthorized use or misuse of AI by our employees or others may result in disclosure of confidential company and customer data, reputational harm, privacy law violations and legal liability. Our use of AI may also lead to novel and urgent cybersecurity risks, including the misuse of personal information, which may adversely affect our operations and reputation. As a result, we may not be able to successfully integrate AI into our products, services and operations despite expending significant time and monetary resources to attempt to do so. Our investments in deploying such technologies may be substantial and may be more expensive than anticipated. If we fail to deploy AI as intended, our competitors may incorporate AI technology into their products or services more successfully than we do, which may impair our ability to effectively compete in the market. Uncertainty in the legal regulatory regime relating to AI may require significant resources to modify and maintain business practices to comply with U. S. and non- U. S. laws, the nature of which cannot be determined at this time. Several jurisdictions around the globe, including Europe and certain U. S. states, have already proposed or enacted laws governing AI. For example, European regulators have proposed a stringent AI regulation, and we expect other jurisdictions will adopt similar laws. Other jurisdictions may decide to adopt similar or more restrictive legislation that may render the use of such technologies challenging. **Additionally, the disclosure and use of personal information in generative AI technologies is subject to various data privacy and security laws and other obligations. Our use of this technology could result in additional compliance costs, regulatory investigations and actions, and consumer lawsuits. Also, we use AI / ML to assist us in making certain decisions, which is regulated by certain privacy laws. Due to inaccuracies or flaws in the inputs, outputs, or logic of the AI / ML, the model could be biased and could lead us to make decisions that could bias certain individuals (or classes of individuals), and adversely impact their rights, employment, and ability to obtain certain pricing, products, services, or benefits.** If we do not or cannot maintain the compatibility of our platform with applications that our customers use, our business could suffer. Some of our customers choose to integrate our solutions with certain other systems used by our customers, such as real- time Technologic, Forensic Logic or SafePointe platforms or computer- aided dispatch systems. The functionality and popularity of our solutions depend, in part, on our ability to integrate our solutions into these systems. Providers of these systems may change the features of their technologies, restrict our access to their applications or alter the terms governing use of their applications in an adverse manner. Such changes could functionally limit or terminate our ability to use these technologies in conjunction with our solutions, which could negatively impact our customer service and harm our business. If we fail to integrate our solutions with applications that our customers use, we may not be able to offer the functionality that our customers need, and our customers may not renew their agreements, which would negatively impact our ability to generate revenues and adversely impact our business. We are in the process of expanding our international operations, which exposes us to significant risks. We currently operate in limited number of locations outside the United States. A key component to our business strategy is to expand our international operations to increase our revenues from customers outside of the United States as part of our growth strategy. Operating in international markets requires significant resources and management attention and will subject us to regulatory, economic and political risks in addition to those we already face in the United States. In addition, we will need to invest time and resources in understanding the regulatory framework and political environments of our potential customers overseas in order to focus our sales efforts. Because such regulatory and political considerations are likely to vary across jurisdictions, this effort will require additional time and attention from our sales team and could lead to a sales cycle that is longer than our typical process for sales in the United States. We also may need to hire additional employees and otherwise invest in our international operations in order to reach new customers. Because of our limited experience with international operations as well as developing and managing sales in international markets, our international expansion efforts may be delayed or may not be successful. In addition, we face and will continue to face risks in doing business internationally that could adversely affect our business, including: • the potential impact of currency exchange fluctuations; • the need to comply with local data residency requirements; • the availability and reliability of local data centers and internet bandwidth providers; • the difficulty of staffing and managing international operations and the increased operations, travel, shipping and compliance costs associated with having customers in numerous international locations; • potentially greater difficulty collecting accounts receivable and longer payment cycles; • the availability and cost of coverage by wireless carriers in international markets; • higher or more variable costs associated with wireless carriers and other service providers; • the need to offer customer support in various languages; • challenges in understanding and complying with local laws, regulations and customs in foreign jurisdictions, including laws regarding privacy and government surveillance; • export controls and economic sanctions administered by the Department of Commerce Bureau of Industry and Security and the Treasury Department' s Office of Foreign Assets Control; • compliance with various anti- bribery and anti- corruption laws such as the Foreign Corrupt Practices Act and United Kingdom Bribery Act of 2010; • tariffs and other non- tariff barriers, such as quotas and local content rules; • more limited protection for our intellectual property in some countries; • adverse or uncertain tax consequences as a result of international operations; • currency control regulations, which might restrict or prohibit our

conversion of other currencies into U. S. dollars; • restrictions on the transfer of funds; • deterioration of political relations between the United States and other countries; and • political or social unrest, global pandemics, or economic instability in a specific country or region in which we operate, which could have an adverse impact on our operations in that location. Also, we expect that due to costs related to our international expansion efforts and the increased cost of doing business internationally, we will incur higher costs to secure sales to international customers than the comparable costs for domestic customers. As a result, our financial results may fluctuate as we expand our operations and customer base worldwide. Our failure to manage any of these risks successfully could harm our international operations, and adversely affect our business, operating results and financial condition. We are dependent on the continued services and performance of our senior management and other key personnel, the loss of any of whom could adversely affect our business. Our future success depends in large part on the continued contributions of our senior management and other key personnel. In particular, the leadership of key management personnel is critical to the successful management of our company, the development of our products, and our strategic direction. We also depend on the contributions of key technical personnel. We do not maintain " key person " insurance for any member of our senior management team or any of our other key employees. Our senior management and key personnel are all employed on an at- will basis, which means that they could terminate their employment with us at any time, for any reason and without notice. The loss of any of our key management personnel could significantly delay or prevent the achievement of our development and strategic objectives and adversely affect our business. If we are unable to attract, integrate and retain additional qualified personnel, including top technical talent, our business could be adversely affected. Our future success depends in part on our ability to identify, attract, integrate and retain highly skilled technical, managerial, sales and other personnel. We face intense competition for qualified individuals from numerous other companies, including other software and technology companies, many of whom have greater financial and other resources than we do. Some of these characteristics may be more appealing to high- quality candidates than those we have to offer. In addition, new hires often require significant training and, in many cases, take significant time before they achieve full productivity. We may incur significant costs to attract and retain qualified personnel, including significant expenditures related to salaries and benefits and compensation expenses related to equity awards, and we may lose new employees to our competitors or other companies before we realize the benefit of our investment in recruiting and training them. Moreover, new employees, especially those who work remotely, may not be or become as productive as we expect, as we may face challenges in adequately or appropriately integrating them into our workforce and culture. If we are unable to attract, integrate and retain suitably qualified individuals who are capable of meeting our growing technical, operational and managerial requirements, on a timely basis or at all, our business will be adversely affected. Volatility or lack of positive performance in our stock price may also affect our ability to attract and retain our key employees. Many of our senior management personnel and other key employees have become, or will soon become, vested in a substantial amount of stock or stock options. Employees may be more likely to leave us if the shares they own or the shares underlying their vested options have significantly appreciated in value relative to the original purchase prices of the shares or the exercise prices of the options, or, conversely, if the exercise prices of the options that they hold are significantly above the market price of our common stock. If we are unable to appropriately incentivize and retain our employees through equity compensation, or if we need to increase our compensation expenses in order to appropriately incentivize and retain our employees, our business, operating results and financial condition would be adversely affected. Legal and Regulatory Risks We **and the third parties with whom we work** are subject to stringent and evolving **U. S. and foreign** laws, ~~governmental regulation~~ **regulations , and rules,** contractual obligations, **industry standards,** policies and other ~~legal~~ obligations ~~,~~ ~~particularly~~ related to data privacy and security. Our **(or the third parties with whom we work)** actual or perceived failure to comply with such obligations could lead to regulatory investigations or actions; litigation (including class claims) and mass arbitration **demands** ; fines and penalties; disruptions of our business operations; ~~reputation~~ **reputational** harm; loss of revenue or profits; loss of customers or sales; and other adverse business consequences. ~~Compliance with such laws could impair our efforts to maintain and expand our customer base, and thereby decrease our revenues.~~ In the ordinary course of business, we process confidential, proprietary, and / or sensitive information, including data collected by our sensors, personal information business data, trade secrets, and intellectual property. Accordingly, our data processing activities ~~are~~ subject **us** to a variety of data privacy and security obligations, such as various laws, regulations, guidance, industry standards, external and internal privacy and security policies, contractual requirements, and other obligations relating to data privacy and security and restrictions on audio monitoring and the **processing** ~~collection, use, storage and disclosure~~ of personal information. In the United States, federal, state, and local governments have enacted numerous data privacy and security laws, including data breach notification laws, **personal data** privacy laws, consumer protection laws (e. g., Section 5 of the Federal Trade Commission Act), and other similar laws (e. g., wiretapping laws). ~~Various~~ **Numerous** U. S. states ~~— including California, Virginia, Colorado, Connecticut, and Utah —~~ have **enacted** ~~adopted and others are considering proposals for~~ comprehensive ~~data~~ privacy ~~and security~~ laws ~~and regulations.~~ that impose certain obligations on covered businesses, including providing specific disclosures in privacy notices and affording residents with certain rights concerning their personal information. ~~,~~ As applicable, such rights may include the right to access, correct ~~and~~ **or** delete certain personal information, and to opt- out of certain data processing activities, such as targeted advertising, profiling, and automated decision- making. The exercise of these rights may impact our business and ability to provide our products and services. **Certain states also impose stricter requirements for processing certain personal information, including sensitive information, such as conducting data privacy impact assessments.** These state laws ~~also~~ allow for statutory fines for noncompliance. For example the California Consumer Privacy Act **of 2018** (" CCPA "), applies to personal information of consumers, business representatives, and employees who are California residents, and requires businesses to provide specific disclosures in privacy notices and honor requests of ~~California residents~~ **such individuals** to exercise certain privacy rights ~~, such as those noted below~~ . The CCPA provides for fines ~~of up to $ 7, 500 per intentional violation~~ and allows private litigants affected by certain data breaches to

recover significant statutory damages. ~~Other similar~~ **Similar** laws are being considered in several other states, as well as at the federal and local levels ~~. These developments further complicate compliance efforts~~ , and ~~increase legal risk and compliance costs for us, and the third parties upon whom~~ we ~~rely~~ **expect more states to pass similar laws in the future** . Outside the United States, an increasing number of laws, regulations, and industry standards govern data privacy and security. For example, the European Union' s General Data Protection Regulation (" EU GDPR "), the United Kingdom' s GDPR (" UK **GDPR ") (collectively, "** GDPR "), Brazil' s General Data Protection Law (Lei Geral de Proteção de Dados Pessoais, or " LGPD ") (Law No. 13, 709 / 2018), and China' s Personal Information Protection Law (" PIPL ") impose strict requirements for processing personal information. For example, under the ~~EU GDPR and UK~~ GDPR, companies may face temporary or definitive bans on data processing and other corrective actions; fines of up to 20 million Euros under the EU GDPR, 17. 5 million pounds sterling under the UK GDPR or, in each case, 4 % of annual global revenue, whichever is greater; or private litigation related to processing of personal information brought by classes of data subjects or consumer protection organizations authorized at law to represent their interests. Additionally, we may be required, under various data privacy and security laws and other obligations, to obtain certain consents to process personal information ~~. Our inability or failure to do so could result in adverse consequences~~ . For example, some of our data processing practices may be challenged under wiretapping laws, if we obtain consumer information from third parties through various methods, including chatbot and session replay providers, or via third- party marketing pixels. These practices may be subject to increased challenges by class action plaintiffs. Our inability or failure to obtain consent for these practices could result in adverse consequences, including class action litigation and mass arbitration demands. **Furthermore, our business relies on the acquisition and sale of personal data, including data obtained from third- party data suppliers.** Regulators are increasingly scrutinizing the activities of **third- party** data suppliers **and acquisition and sale of personal data from or to third parties** , and laws in the United States (including the CCPA and California' s Delete Act) and other jurisdictions **, such as Europe (including through the GDPR and the ePrivacy Directive),** are likewise regulating such activity. These laws ~~, which may apply to us and our partners,~~ pose additional, material compliance risks to **such** data suppliers, and **these** suppliers may not be able to provide **us with** personal information in compliance with these laws. For example, some data suppliers are required to register as data brokers under California and Vermont law and file reports with regulators, which exposes them to increased scrutiny. Additionally, California' s Delete Act requires ~~a regulatory~~ **the California Privacy Protection** ~~agency~~ **Agency** to establish by January 1, 2026 a mechanism to allow California consumers to submit a single, verifiable request to delete all of their personal information held by all registered data brokers and their service providers. Moreover, data suppliers have recently been subject to increased litigation under various claims of violating certain state privacy laws. These laws and ~~related~~ challenges may make it so difficult for us or our suppliers to provide the data that the costs associated with the data materially increase or may materially decrease the availability of data that data suppliers can provide. **Obtaining and selling personal data from third parties carries risk to us. For example, we have registered as a data broker and file reports with certain regulators, which exposes us to increased scrutiny.** In addition, we may face compliance risks and limitations on our ability to use certain data provided by our ~~data~~ **third- party** suppliers if those suppliers have not complied with applicable privacy laws, provided appropriate notice to data subjects, obtained necessary consents, or established a legal basis for the transfer and processing of the data by us. ~~Our employees and personnel~~ **These challenges may make it so difficult for** ~~use~~ -- **us** ~~generative AI technologies~~ **and our suppliers** to ~~perform~~ **provide** ~~their~~ -- **the** ~~work, and the disclosure and use of personal information in generative AI technologies is subject to various~~ data ~~privacy~~ and ~~security laws and other~~ -- **the** ~~obligations. Governments have passed and are likely to pass additional laws regulating generative AI. Our use of this technology could result in additional compliance~~ costs **associated with the** ~~, regulatory investigations and actions, and consumer lawsuits. If we are unable to use generative AI, it could make our business less efficient and result in competitive disadvantages. We use AI / ML to assist us in making certain decisions, which is regulated by certain~~ data **materially increase** ~~privacy and security laws. Due to inaccuracies~~ or ~~flaws in~~ **may materially decrease** the **availability** ~~inputs, outputs, or logic~~ of **data** ~~the AI / ML, the model could be biased and could lead us to make decisions~~ that **we or** ~~could bias certain individuals (or~~ **our data suppliers can provide** ~~classes of individuals), and adversely impact their rights, employment, and ability to obtain certain pricing, products, services, or benefits~~ . We are also bound by contractual obligations related to data privacy and security, and our efforts to comply with such obligations may not be successful. For example, certain ~~data~~ privacy ~~and security~~ laws, such as the GDPR and the CCPA, require our customers to impose specific contractual restrictions on their service providers. We publish privacy policies, marketing materials **, whitepapers,** and other statements, such as **statements related to** compliance with certain certifications or self- regulatory principles, ~~regarding~~ **concerning** data privacy ~~and~~ **,** security **, and AI** . ~~If~~ **Regulators in the United States are increasingly scrutinizing these statements, and if** these policies, materials or statements are found to be deficient, lacking in transparency, deceptive, unfair **, misleading** , or misrepresentative of our practices, we may be subject to investigation, enforcement actions by regulators or other adverse consequences. Obligations related to data privacy and security (and consumers' data privacy and security expectations) are quickly changing, becoming increasingly stringent, and creating uncertainty. Additionally, these obligations may be subject to differing applications and interpretations, which may be inconsistent or conflict among jurisdictions. Preparing for and complying with these obligations requires us to devote significant resources, which may necessitate changes to our services, information technologies, systems, and practices and to those of any third parties that process personal information on our behalf. In addition, these obligations may require us to change our business model. We may at times fail (or be perceived to have failed) in our efforts to comply with our data privacy and security obligations. Moreover, despite our efforts, our personnel or third parties ~~on~~ **with** whom we ~~rely~~ **work** may fail to comply with such obligations, which could negatively impact our business operations. If we or the third parties ~~on which~~ **with whom** we ~~rely~~ **work** fail, or are perceived to have failed, to address or comply with applicable data privacy and security obligations, we could face significant consequences, including but not limited to: government enforcement actions (e. g., investigations, fines, penalties, audits, inspections, and similar); litigation (including class- action claims **)** and mass arbitration

demands ~~)~~; additional reporting requirements and / or oversight; bans **or restrictions** on processing personal information; orders to destroy or not use personal information; and imprisonment of company officials. In particular, plaintiffs have become increasingly more active in bringing ~~data~~ privacy- related claims against companies, including class claims and mass arbitration demands. Some of these claims allow for the recovery of statutory damages on a per violation basis, and, if viable, carry the potential for monumental statutory damages, depending on the volume of data and the number of violations. Any of these events could have a material adverse effect on our reputation, business, or financial condition, including but not limited to: loss of customers; interruptions or stoppages in our business operations; inability to process personal information or to operate in certain jurisdictions; limited ability to develop or commercialize our products; expenditure of time and resources to defend any claim or inquiry; adverse publicity; or substantial changes to our business model or operations. We may be subject to additional obligations to collect and remit certain taxes, and we may be subject to tax liability for past activities, which could harm our business. State, local and foreign jurisdictions have differing rules and regulations governing sales, use, value added and other taxes, and these rules and regulations are subject to varying interpretations that may change over time, particularly with respect to software- as- a- service products like our solutions. Further, these jurisdictions' rules regarding tax nexus are complex and vary significantly. If one or more jurisdictions were to assert that we have failed to collect taxes for sales of our solutions, we could face the possibility of tax assessments and audits. A successful assertion that we should be collecting additional sales, use, value added or other taxes in those jurisdictions where we have not historically done so and do not accrue for such taxes could result in substantial tax liabilities and related penalties for past sales or otherwise harm our business and operating results. Our ability to use our net operating losses to offset future taxable income may be subject to certain limitations. As of December 31, ~~2023~~ **2024**, we had federal net operating loss carryforwards (" NOLs ") of approximately $ ~~57~~ **50**. ~~9~~ **0** million, of which $ ~~53~~ **45**. 1 million will begin to expire in ~~2029~~ **2030**, if not utilized. The remaining net operating losses of $ 4. 9 million can be carried forward indefinitely under the Tax Cuts and Jobs Act. As of December 31, ~~2023~~ **2024**, we also had state NOLs of approximately $ ~~42~~ **41**. ~~7~~ **5** million, which begin expiring in ~~2024~~ **2025**. These federal and state NOLs may be available to reduce future income subject to income taxes. In general, under Section 382 of the Internal Revenue Code of 1986, as amended (~~"~~ the **"** Code ~~"~~ **"**), a corporation that undergoes an " ownership change " is subject to limitations on its ability to utilize its NOLs to offset future taxable income. Past or future changes in our stock ownership, some of which are outside of our control, may have resulted or could result in an ownership change. State NOLs generated in one state cannot be used to offset income generated in another state. In addition, at the state level, there may be periods during which the use of NOLs is suspended or otherwise limited, such as the 2020 temporary suspension of the ability to use California NOLs and limitation on the use of certain tax credits to offset California income and tax liabilities, which could accelerate or permanently increase state taxes owed. We may be subject to litigation for a variety of claims or to other legal requests, which could adversely affect our results of operations, harm our reputation or otherwise negatively impact our business. We may be subject to litigation for a variety of claims arising from our normal business activities. These may include claims, suits, and proceedings involving labor and employment, wage and hour, commercial and other matters. The outcome of any litigation, regardless of its merits, is inherently uncertain. Any claims and lawsuits, and the disposition of such claims and lawsuits, could be time- consuming and expensive to resolve, divert management attention and resources, and lead to attempts on the part of other parties to pursue similar claims. Any adverse determination related to litigation could adversely affect our results of operations, harm our reputation or otherwise negatively impact our business. In addition, depending on the nature and timing of any such dispute, a resolution of a legal matter could materially affect our future operating results, our cash flows or both. An unfavorable outcome on any litigation matters could require us to pay substantial damages, or, in connection with any intellectual property infringement claims, could require us to pay ongoing royalty payments or could prevent us from selling certain of our products. As a result, a settlement of, or an unfavorable outcome on, any of the matters referenced above or other litigation matters could have a material adverse effect on our business, operating results, financial condition and cash flows. We, or our customers, may be subject to requests for our data or information concerning our techniques and processes, pursuant to state or federal law (for example, public- records requests or subpoenas to provide information or to testify in court). This data and information, some of which we may deem to be confidential or trade secrets, could therefore become a matter of public record and also become accessible by competitors, which could negatively impact our business. Changes in financial accounting standards may cause adverse and unexpected revenue fluctuations and impact our reported results of operations. The accounting rules and regulations that we must comply with are complex and subject to interpretation by the Financial Accounting Standards Board, the Securities and Exchange Commission and various bodies formed to promulgate and interpret appropriate accounting principles. In addition, many companies' accounting disclosures are being subjected to heightened scrutiny by regulators and the public. Further, the accounting rules and regulations are continually changing in ways that could impact our financial statements. Changes to accounting principles or our accounting policies on our financial statements going forward are difficult to predict, could have a significant effect on our reported financial results, and could affect the reporting of transactions completed before the announcement of the change. In addition, were we to change our critical accounting estimates, including the timing of recognition of subscription and professional services revenues and other revenues sources, our results of operations could be significantly impacted. Failure to protect our intellectual property rights could adversely affect our business. Our success depends, in part, on our ability to protect proprietary methods and technologies that we develop or license under patent and other intellectual property laws of the United States, as well as our brands, so that we can prevent others profiting from them. We rely on a combination of contractual and intellectual property rights, including non- disclosure agreements, patents, trade secrets, copyrights and trademarks, to establish and protect our intellectual property rights in our names, services, innovations, methodologies and related technologies. If we fail to protect our intellectual property rights adequately, our competitors might gain access to our technology and our business might be adversely affected. As of December 31, ~~2023~~ **2024**, we had 34 issued patents directed to our technologies, ~~27~~ **28** in the United States, two in Brazil, one each in Israel, Mexico, the United Kingdom,

France and Germany. The issued patents expire on various dates from ~~2023~~ **2025** to 2034. We have patent applications pending for examination in the United States, Europe, Mexico and Brazil, but we cannot guarantee that these patent applications will be granted. We also license one other U. S. patent from one third party **which expired in November 2023** . The patents that we own or those that we license from others (including those that may be issued in the future) may not provide us with any competitive advantages or may be challenged by third parties. The process of obtaining patent protection is expensive and time-consuming, and we may not be able to prosecute all necessary or desirable patent applications at a reasonable cost or in a timely manner. Even if issued, there can be no assurance that these patents will adequately protect our intellectual property, as the legal standards relating to the validity, enforceability and scope of protection of patent and other intellectual property rights are uncertain. Any patents that are issued may subsequently be invalidated or otherwise limited, allowing other companies to develop offerings that compete with ours, which could adversely affect our competitive business position, business prospects and financial condition. In addition, issuance of a patent does not guarantee that we have a right to practice the patented invention. Patent applications in the United States are typically not published until 18 months after their earliest priority date or, in some cases, not at all, and publications of discoveries in industry- related literature lag behind actual discoveries. We cannot be certain that third parties do not have blocking patents that could be used to prevent us from marketing or practicing our software or technology. Effective patent, trademark, copyright and trade secret protection may not be available to us in every country in which our software is available. The laws of some foreign countries may not be as protective of intellectual property rights as those in the United States (in particular, some foreign jurisdictions do not permit patent protection for software), and mechanisms for enforcement of intellectual property rights may be inadequate. Additional uncertainty may result from changes to intellectual property legislation enacted in the United States, including the recent America Invents Act, or to the laws of other countries and from interpretations of the intellectual property laws of the United States and other countries by applicable courts and agencies. Accordingly, despite our efforts, we may be unable to prevent third parties from infringing upon or misappropriating our intellectual property. We rely in part on trade secrets, proprietary know- how and other confidential information to maintain our competitive position. Although we endeavor to enter into non- disclosure agreements with our employees, licensees and others who may have access to this information, we cannot assure you that these agreements or other steps we have taken will prevent unauthorized use, disclosure or reverse engineering of our technology. Moreover, third parties may independently develop technologies or products that compete with ours, and we may be unable to prevent this competition. Third parties also may seek access to our trade secrets, proprietary know- how and other confidential information through legal measures (for example, public- records requests or subpoenas to provide information or to testify in court) and it could be expensive to defend against those requests. Disclosure of our trade secrets, proprietary know- how and other confidential information could negatively impact our business. We might be required to spend significant resources to monitor and protect our intellectual property rights. We may initiate claims or litigation against third parties for infringement of our proprietary rights or to establish the validity of our proprietary rights. We may also engage in litigation in response to public- records requests or subpoenas that seek our intellectual property. Litigation also puts our patents at risk of being invalidated or interpreted narrowly and our patent applications at risk of not issuing. Additionally, we may provoke third parties to assert counterclaims against us. We may not prevail in any lawsuits that we initiate or other legal proceedings in which we participate, and the damages or other remedies awarded, if any, may not be commercially viable. Any litigation, whether or not resolved in our favor, could result in significant expense to us and divert the efforts of our technical and management personnel, which may adversely affect our business, operating results, financial condition and cash flows. We may be subject to intellectual property rights claims by third parties, which are extremely costly to defend, could require us to pay significant damages and could limit our ability to use certain technologies. Companies in the software and technology industries, including some of our current and potential competitors, own large numbers of patents, copyrights, trademarks and trade secrets and frequently enter into litigation based on allegations of infringement or other violations of intellectual property rights. In addition, many of these companies have the capability to dedicate substantially greater resources to enforce their intellectual property rights and to defend claims that may be brought against them. The litigation may involve patent holding companies or other adverse patent owners that have no relevant product revenues and against which our patents may therefore provide little or no deterrence. We may have previously received, and may in the future receive, notices that claim we have misappropriated, misused, or infringed other parties' intellectual property rights, and, to the extent we gain greater market visibility, we face a higher risk of being the subject of intellectual property infringement claims. There may be third- party intellectual property rights, including issued or pending patents that cover significant aspects of our technologies or business methods. Any intellectual property claims, with or without merit, could be very time- consuming, could be expensive to settle or litigate and could divert our management' s attention and other resources. These claims could also subject us to significant liability for damages, potentially including treble damages if we are found to have willfully infringed patents or copyrights. These claims could also result in our having to stop using technology found to be in violation of a third party' s rights. We might be required to seek a license for the intellectual property, which may not be available on a timely basis, on reasonable terms or at all. We also may be required to modify our products, services, internal systems or technologies. Even if a license were available, we could be required to pay significant royalties, which would increase our operating expenses. As a result, we may be required to develop alternative non- infringing technology, which could require significant effort and expense. If we cannot license or develop technology for any infringing aspect of our business, we would be forced to limit or stop sales of our software and may be unable to compete effectively. Any of these results would adversely affect our business, operating results, financial condition and cash flows. Our use of generative artificial intelligence tools may pose particular risks to our proprietary software and systems and subject us to legal liability. We use generative AI tools in our business, including to generate code and other materials incorporated with our proprietary software and systems, and expect to use generative AI tools in the future. Generative AI tools producing content which can be indistinguishable from that generated by humans is a relatively novel development, with benefits, risks, and liabilities still

unknown. Recent decisions of the U. S. Copyright Office suggest that we would not be able to claim copyright ownership in any source code, text, images, or other materials, which we develop through use of generative AI tools, and the availability of such protections in other countries is unclear. As a result, we could have no remedy if third parties reused those same materials, or similar materials also generated by AI tools. We also face risks to any confidential or proprietary information of the Company which we may include in any prompts or inputs into any generative AI tools, as the providers of the generative AI tools may use these inputs or prompts to further train the tools. Not all providers offer an option to opt- out of such usage, and, even where we do opt- out, we cannot guarantee that the opt- out will be fully effective. In addition, we have little or no insight into the third- party content and materials used to train these generative AI tools, or the extent of the original works which remain in the outputs. As a result, we may face claims from third parties claiming infringement of their intellectual property rights, or mandatory compliance with open source software or other license terms, with respect to software, or other materials or content we believed to be available for use, and not subject to license terms or other third- party proprietary rights. We could also be subject to claims from the providers of the generative AI tools, if we use any of the generated materials in a manner inconsistent with their terms of use. Any of these claims could result in legal proceedings and could require us to purchase a costly license, comply with the requirement of open source software license terms, or limit or cease using the implicated software, or other materials or content unless and until we can re- engineer such software, materials, or content to avoid infringement or change the use of, or remove, the implicated third- party materials, which could reduce or eliminate the value of our technologies and services. Our use of generative AI tools may also present additional security risks because the generated source code may have been modelled from publicly available code, or otherwise not subject to all of our standard internal controls, which may make it easier for hackers and other third parties to determine how to breach our website and systems that rely on the code. Any of these risks could be difficult to eliminate or manage, and, if not addressed, could have a material adverse effect on our business, results of operations, financial condition, and future prospects. Our use of open source software could subject us to possible litigation. A portion of our technologies incorporates open source software, and we expect to continue to incorporate open source software into our platform in the future. Few of the licenses applicable to open source software have been interpreted by courts, and their application to the open source software integrated into our proprietary technology platform may be uncertain. If we fail to comply with these licenses, then pursuant to the terms of these licenses, we may be subject to certain requirements, including requirements that we make available the source code for our software that incorporates the open source software. We cannot assure you that we have not incorporated open source software in our software in a manner that is inconsistent with the terms of the applicable licenses or our current policies and procedures. If an author or other third party that distributes such open source software were to allege that we had not complied with the conditions of one or more of these licenses, we could incur significant legal expenses defending against such allegations. Litigation could be costly for us to defend, have a negative effect on our operating results and financial condition or require us to devote additional research and development resources to change our technology platform. Risks Related to the Ownership of Our Common Stock **We have identified a material weakness in our internal control over financial reporting as of December 31, 2024. If we are unable to develop and maintain an effective system of internal control over financial reporting, we may not be able to accurately report our financial results in a timely manner, which may adversely affect investor confidence in us and materially and adversely affect our business and operating results. A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting such that there is a reasonable possibility that a material misstatement of our annual or interim financial statements will not be prevented, or detected and corrected on a timely basis. Effective internal controls are necessary for us to provide reliable financial reports and prevent fraud. Under the supervision of and with the participation of our management, we assessed the effectiveness of our internal control over financial reporting as of December 31, 2024, using the criteria set forth by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in Internal Control — Integrated Framework (2013). Based on management' s assessment of our internal control over financial reporting, under the criteria described in the preceding sentence, management has identified a material weakness in internal control during the year ended December 31, 2024. See Part II, Item 9A, " Controls and Procedures " of this report. If we are unable to develop and maintain an effective system of internal control over financial reporting, we may not be able to accurately report our financial results in a timely manner, which may adversely affect investor confidence in us and materially and adversely affect our business and operating results. We cannot assure you that there will not be additional material weaknesses or significant deficiencies in our internal control over financial reporting in the future. Any failure to maintain internal control over financial reporting could severely inhibit our ability to accurately report our financial condition, results of operations or cash flows. If we are unable to conclude that our internal control over financial reporting is effective, or if our independent registered public accounting firm determines we have a material weakness in our internal control over financial reporting, investors may lose confidence in the accuracy and completeness of our financial reports, the market price of our common stock could decline, and we could be subject to sanctions or investigations by Nasdaq, the SEC or other regulatory authorities. Failure to remedy any material weakness in our internal control over financial reporting, or to implement or maintain other effective control systems required of public companies, could also restrict our future access to the capital markets. Management has been implementing and continues to implement measures to remediate the material weakness. These remediation measures may be time consuming and costly and there is no assurance that these initiatives will ultimately have the intended effects. If we identify any new material weaknesses in the future, any such newly identified material weakness could limit our ability to prevent or detect a misstatement of our accounts or disclosures that could result in a material misstatement of our annual or interim financial statements. In such case, we may be unable to maintain compliance with securities law requirements regarding timely filing of periodic reports in addition to applicable stock exchange listing requirements, investors may lose confidence in our financial reporting and our stock price may decline**

as a result. We cannot assure you that the measures we have taken to date, or any measures we may take in the future, will be sufficient to avoid potential future material weaknesses. Our stock price may be volatile or may decline regardless of our operating performance, resulting in substantial losses for investors. The market price of our common stock has fluctuated and may continue to fluctuate significantly in response to numerous factors, many of which are beyond our control, including the factors listed below and other factors described in this " Risk Factors " section: • actual or anticipated fluctuations in our operating results; • 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 by any securities analysts who follow our company, or our failure to meet these estimates or the expectations of investors; • ratings changes by any securities analysts who follow our company; • changes in the availability of federal funding to support local law enforcement efforts, or local budgets; • announcements by us of significant technical innovations, acquisitions, strategic partnerships, joint ventures or capital commitments; • changes in operating performance and stock market valuations of other software companies generally; • price and volume fluctuations in the overall stock market, including as a result of trends in the economy as a whole; • changes in our board of directors or management; • sales of large blocks of our common stock, including sales by our executive officers, directors and significant stockholders; • lawsuits threatened or filed against us; • novel and unforeseen market forces and trading strategies, as well as short sales, hedging and other derivative transactions involving our capital stock; • the impact of past and potential future disruptions in access to bank deposits and lending commitments due to bank failures, and other macroeconomic pressures; • general economic conditions in the United States and abroad; • other events or factors, including those resulting from pandemics, protests against racial inequality, protests against police brutality and movements such as " Defund the Police, " war, incidents of terrorism or responses to these events; and • negative publicity, including false information, regarding our solutions. In addition, stock markets have experienced extreme price and volume fluctuations that have affected and continue to affect the market prices of equity securities of many software companies. Stock prices of many software companies have fluctuated in a manner unrelated or disproportionate to the operating performance of those companies. Broad market and industry fluctuations, as well as general economic, political, regulatory and market conditions, may negatively impact the market price of our common stock. In the past, stockholders have instituted securities action litigation following periods of market volatility. If we were to become involved in securities litigation, it could subject us to substantial costs, divert resources and the attention of management from our business and adversely affect our business, operating results, financial condition and cash flows. Substantial future sales of shares of our common stock could cause the market price of our common stock to decline. Non- affiliates have the ability to sell shares of our common stock in the open market or through block trades without being subject to volume restrictions under Rule 144 of the Securities Act. In addition, in the future we may issue common stock or other securities if we need to raise additional capital. The number of new shares of our common stock issued in connection with raising additional capital could constitute a material portion of the then outstanding shares of our common stock. In the event a large number of shares of common stock are sold in the public market, such share sales could reduce the trading price of our common stock. Stock repurchases could increase the volatility of the trading price of our common stock and diminish our cash reserves, and we cannot guarantee that our stock repurchase program will enhance long- term stockholder value. In November 2022, our board of directors approved a new stock repurchase program for up to $ 25. 0 million of our common stock, of which $ ~~5~~ **11** . 6 million was utilized as of December 31, ~~2023~~ **2024** . Although our board of directors has authorized the stock repurchase program, it does not obligate us to repurchase any specific dollar amount or number of shares, there is no expiration date for the stock repurchase program, and the stock repurchase program may be modified, suspended or terminated at any time and for any reason. The timing and actual number of shares repurchased under the stock repurchase program will depend on a variety of factors, including the acquisition price of the shares, our liquidity position, general market and economic conditions, legal and regulatory requirements and other considerations. Our ability to repurchase shares may also be limited by restrictive covenants in our existing credit agreement or in future borrowing arrangements we may enter into from time to time. Repurchases of our shares could increase the volatility of the trading price of our stock, which could have a negative impact on the trading price of our stock. Similarly, the future announcement of the termination or suspension of the stock repurchase program, or our decision not to utilize the full authorized repurchase amount under the stock repurchase program, could result in a decrease in the trading price of our stock. In addition, the stock repurchase program could have the impact of diminishing our cash reserves, which may impact our ability to finance our growth, complete acquisitions and execute our strategic plan. There can be no assurance that any share repurchases we do elect to make will enhance stockholder value because the market price of our common stock may decline below the levels at which we repurchased our shares. Although our stock repurchase program is intended to enhance long- term stockholder value, we cannot guarantee that it will do so and short- term stock price fluctuations could reduce the effectiveness of the stock repurchase program. If securities or industry analysts do not publish research or reports about our business, or publish negative reports about our business, our share price and trading volume could decline. The trading market for our common stock depends in part on the research and reports that securities or industry analysts publish about us or our business, our market and our competitors. We do not have any control over these analysts. If one or more of the analysts who cover us downgrade our shares of common stock or change their opinion of our shares of common stock, our share price would likely decline. If one or more of these analysts cease coverage of our company or fail to regularly publish reports on us, we could lose visibility in the financial markets, which could cause our share price or trading volume to decline. We incur substantial costs as a result of being a public company. As a public company, we are incurring significant levels of legal, accounting, insurance and other expenses that we did not incur as a private company. We are subject to the reporting requirements of the Exchange Act, the Sarbanes- Oxley Act, the Dodd- Frank Act, the listing requirements of the Nasdaq Capital Market, and other applicable securities rules and regulations. Compliance with these rules and regulations increases our legal and financial compliance costs, makes some activities more difficult, time- consuming or costly and increases demand on our systems and resources as compared to when we

operated as a private company. The Exchange Act requires, among other things, that we file annual, quarterly and current reports with respect to our business and operating results. The Sarbanes- Oxley Act requires, among other things, that we maintain effective disclosure controls and procedures and internal control over financial reporting. In order to maintain and, if required, improve our disclosure controls and procedures and internal control over financial reporting to meet this standard, significant resources and management oversight may be required **. Furthermore, if any issues in complying with those requirements are identified (for example, our recent identification of a material weakness over our internal controls over financial reporting and any additional material weaknesses or significant deficiency in the internal control over financial reporting that we or our independent registered public accounting firm may identify in the future), we could incur additional costs rectifying those issues, and the existence of those issues could adversely affect our reputation or investor perceptions of it** . As a result, management' s attention may be diverted from other business concerns, which could adversely affect our business and operating results. Although we have already hired additional corporate employees to comply with these requirements, we may need to hire more corporate employees in the future or engage outside consultants, which would increase our costs and expenses. In addition, changing laws, regulations and standards relating to corporate governance and public disclosure are creating uncertainty for public companies, increasing legal and financial compliance costs and making some activities more time- consuming. These laws, regulations and standards are subject to varying interpretations, in many cases due to their lack of specificity, and, as a result, their application in practice may evolve over time as new guidance is provided by regulatory and governing bodies. This could result in continuing uncertainty regarding compliance matters and higher costs necessitated by ongoing revisions to disclosure and governance practices. We ~~intend to~~ invest resources to comply with evolving laws, regulations and standards, and ~~this~~ **these** ~~investment~~ **investments** may result in increased **operating** ~~general and administrative~~ expenses and a diversion of management' s time and attention from revenue- generating activities to compliance activities. If our efforts to comply with new laws, regulations and standards differ from the activities intended by regulatory or governing bodies due to ambiguities related to their application and practice, regulatory authorities may initiate legal proceedings against us and our business may be adversely affected. As a result of disclosure of information in this report and in the filings that we are required to make as a public company, our business, operating results and financial condition have become more visible, which has resulted in, and may in the future result in threatened or actual litigation, including by competitors and other third parties. If any such claims are successful, our business, operating results and financial condition could be adversely affected, and 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 adversely affect our business, operating results and financial condition. We do not intend to pay dividends for the foreseeable future. We have never declared or paid any cash dividends on our common stock and do not intend to pay any cash dividends in the foreseeable future. We anticipate that we will retain all of our future earnings for use in the development of our business and for general corporate purposes. Any determination to pay dividends in the future will be at the discretion of our board of directors. Accordingly, investors must rely on sales of their common stock after price appreciation, which may never occur, as the only way to realize any future gains on their investments. Anti- takeover provisions in our charter documents and under Delaware law could make an acquisition of our company more difficult, limit attempts by our stockholders to replace or remove our current management and limit the market price of our common stock. Provisions in our certificate of incorporation and bylaws may have the effect of delaying or preventing a change of control or changes in our management. Our certificate of incorporation and bylaws include provisions that: • establish a classified board of directors so that not all members of our board of directors are elected at one time; • permit the board of directors to establish the number of directors and fill any vacancies and newly- created directorships; • provide that directors may only be removed for cause; • require super- majority voting to amend some provisions in our certificate of incorporation and bylaws; • authorize the issuance of " blank check " preferred stock that our board of directors could use to implement a stockholder rights plan; • eliminate the ability of our stockholders to call special meetings of stockholders; • prohibit stockholder action by written consent, which requires all stockholder actions to be taken at a meeting of our stockholders; • provide that the board of directors is expressly authorized to make, alter or repeal our bylaws; and • establish advance notice requirements for nominations for election to our board of directors or for proposing matters that can be acted upon by stockholders at annual stockholder meetings. In addition, we are governed by the provisions of Section 203 of the Delaware General Corporation Law, which generally prohibits stockholders owning 15 % or more of our outstanding voting stock from merging or otherwise combining with us for a period of three years following the date on which the stockholder became a 15 % stockholder without the consent of our board of directors. These provisions may frustrate or prevent any attempts by our stockholders to replace or remove our current management by making it more difficult for stockholders to replace members of our board of directors, which is responsible for appointing the members of our management, and otherwise discourage management takeover attempts. Our certificate of incorporation contains exclusive forum provisions that could limit our stockholders' ability to obtain a favorable judicial forum for disputes with us. Pursuant to our certificate of incorporation, unless we consent in writing to the selection of an alternative forum, the Court of Chancery of the State of Delaware is the sole and exclusive forum for (1) any derivative action or proceeding brought on our behalf, (2) any action asserting a claim of breach of a fiduciary duty owed by any of our directors, officers or other employees to us or our stockholders, (3) any action asserting a claim arising pursuant to any provision of the Delaware General Corporation Law, our certificate of incorporation or our bylaws or (4) any action asserting a claim governed by the internal affairs doctrine. Our certificate of incorporation further provides that any person or entity purchasing or otherwise acquiring any interest in shares of our common stock is deemed to have notice of and consented to the foregoing provision. Our certificate of incorporation further provides that the federal district courts of the United States of America will be the exclusive forum for resolving any complaint asserting a cause of action arising under the Securities Act. These forum selection clauses in our certificate of incorporation may limit our stockholders' ability to obtain a favorable judicial forum for disputes with us. While the Delaware courts have determined that such choice of forum provisions

are facially valid and several state trial courts have enforced such provisions and required that suits asserting Securities Act claims be filed in federal court, there is no guarantee that courts of appeal will affirm the enforceability of such provisions and a stockholder may nevertheless seek to bring a claim in a venue other than those designated in the exclusive forum provisions. In such instance, we would expect to vigorously assert the validity and enforceability of the exclusive forum provisions of our certificate of incorporation. This may require significant additional costs associated with resolving such action in other jurisdictions and there can be no assurance that the provisions will be enforced by a court in those other jurisdictions. If a court were to find either exclusive forum provision in our certificate of incorporation to be inapplicable or unenforceable in an action, we may incur further significant additional costs associated with litigating Securities Act claims in state court, or both state and federal court, which could seriously harm our business, financial condition, results of operations, and prospects. ~~55~~ **58**