

Risk Factors Comparison 2024-03-15 to 2023-03-23 Form: 10-K

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

A description of the risks and uncertainties associated with our business and industry is set forth below. You should carefully consider the risks and uncertainties described below, together with all of the other information in this Annual Report on Form 10- K, including our consolidated financial statements and notes thereto and the “ Management’ s discussion and analysis of financial condition and results of operations ” section of Annual Report on Form 10- K, before deciding whether to purchase shares of our common stock. If any of the following risks are realized, our business, financial condition, operating results and prospects could be materially and adversely affected. In that event, the price of our common stock could decline, perhaps significantly. Additional risks and uncertainties not presently known to us or that we currently deem immaterial also may impair our business operations. Certain statements in this Annual Report on Form 10- K are forward- looking statements. See the section of this Annual Report on Form 10- K titled “ Special Note Regarding Forward- Looking Statements. ” Risks relating to our business and industry We have grown rapidly in recent periods, and as a result, our expenses have continued to increase. If we fail to manage our growth effectively, our revenue may not increase, and we may be unable to implement our business strategy. We have experienced significant growth in recent periods, which puts strain on our business, operations and employees. We anticipate that our operations will continue to expand. As we continue to grow, both organically and through acquisitions, we must effectively integrate, develop, and manage an increasingly distributed employee base in a fully remote working environment. We may find it challenging to maintain the same level of employee productivity while executing our growth plan, fostering collaboration, and maintaining the beneficial aspects of our culture, and any such failures could negatively affect our future success, including our ability to attract and retain highly qualified employees and to achieve our business objectives. In addition, to manage our current and anticipated future growth effectively, we must continue to maintain and enhance our IT infrastructure, financial and accounting systems and controls and continue to build our qualified work force in key areas of our company. A key element of how we manage our growth is our ability to scale our capabilities and satisfactorily implement **solutions** ~~the Phreesia Platform~~ for our clients’ needs. Our healthcare services clients often require specific features or functions unique to their organizational structure, which, at a time of significant growth or during periods of high demand, may strain our implementation capacity and hinder our ability to successfully implement **our solutions for the Phreesia Platform** to our clients in a timely manner. If we are unable to address the needs of our healthcare services clients or our healthcare services clients are unsatisfied with the quality of **our solutions** ~~the Phreesia Platform~~ or our services due to our inability to manage our rapid growth, they may not renew their contracts, seek to cancel or terminate their relationship with us or renew on less favorable terms, any of which could adversely affect our business. Failure to effectively manage our growth could also lead us to over- invest or under- invest in development and operations, result in weaknesses in our infrastructure, systems or controls, give rise to operational mistakes, financial losses, loss of productivity or business opportunities and result in loss of employees and reduced productivity of remaining employees. In addition, our growth has required and is expected to require significant capital expenditures and may divert financial resources from other projects such as the development of new applications and services. We may also need to make further investments in our technology and automate portions of **our solutions** ~~the Phreesia Platform~~ or our services to decrease our costs. If our management is unable to effectively manage our growth, our revenue may not increase (including sufficiently to offset our expenses) or may grow more slowly than expected and we may be unable to implement our business strategy. We operate in a highly competitive industry, and if we are not able to compete effectively, including with the EHR and PM systems with which we integrate, our business and results of operations will be harmed. The market for our products and services is fragmented, competitive and characterized by rapidly evolving technology standards, evolving regulatory requirements, changes in client needs and the frequent introduction of new products and services. Our competitors range from smaller niche companies to large, well- financed and technologically- sophisticated entities, including the EHR and PM systems with which we integrate. As costs fall and technology improves, increased market saturation may change the competitive landscape in favor of competitors with greater scale than we currently possess. In order to remain competitive, we are continually involved in a number of projects to compete with new market entrants by developing new services, growing our client base and penetrating new markets. These projects carry risks, such as cost overruns, delays in delivery, performance problems and lack of acceptance by our clients. The success of our business and growth strategy depend upon our continued ability to maintain and expand a network of healthcare services clients. If we are unable to attract and retain healthcare services clients, it would have a material adverse effect on our business and ability to grow and would adversely affect our results of operations. Our success also depends on providing high- quality products and services that healthcare services clients use to improve clinical, financial and operational performance and that are used and positively received by patients. If we cannot adapt to rapidly evolving industry standards and technology and increasingly sophisticated and varied healthcare services organization and patient needs, our existing technology could become undesirable, obsolete or harm our reputation. We believe demand for our products and services has been driven in large part by increasing patient responsibility, engagement and consumerism. Our ability to streamline the intake process and critical workflows in order to improve healthcare services organization, staff efficiency and patient engagement to allow for optimal allocation of resources will be critical to our business. Our success also depends on the ability of our ~~Platform~~ **solutions** to increase patient engagement, and our ability to demonstrate the value of our ~~Platform~~ **solutions** to healthcare services clients, patients and life sciences companies. If our existing clients do not recognize or acknowledge the benefits of our ~~solutions Platform or our~~ **or Platform does our solutions do** not drive patient engagement, then the market for our products and services might develop more slowly than we expect,

which could adversely affect our operating results. In addition, as we and the EHR and PM solutions with which we integrate, grow and expand product offerings, the EHR and PM solutions with which we integrate could offer more competitive services. Some of these EHR and PM systems offer, or may begin to offer, services, including patient intake and engagement services, payment processing tools and direct patient communication services, in the same or similar manner as we do. Although there are many potential opportunities for, and applications of, these services, these EHR and PM systems may seek opportunities or target new clients in areas that may overlap with those that we have chosen to pursue. Such competition from these EHR and PM systems may adversely affect our business, market share and results from operations. We compete on the basis of several factors, including breadth, depth and quality of product and service offerings, ability to deliver clinical, financial and operational performance improvement through the use of products and services, quality and reliability of services, ease of use and convenience, brand recognition, price and the ability to integrate our Platform solutions with various EHR and PM systems and other technology. Some of our competitors have greater name recognition, longer operating histories and significantly greater resources than we do. As a result, our competitors may be able to respond more quickly and effectively than we can to new or changing opportunities, technologies, standards or client requirements. In addition, current and potential competitors have established, and may in the future establish, cooperative relationships with vendors of complementary products, technologies or services to increase the availability of their products to the marketplace. Accordingly, new competitors or providers of EHR and PM solutions may emerge that have greater market share, larger client bases, more widely adopted proprietary technologies, greater marketing expertise, greater financial resources and larger sales forces than we have, which could put us at a competitive disadvantage. We also may be subject to pricing pressures as a result of, among other things, competition within the industry, consolidation of healthcare industry participants, practices of managed care organizations, government action and financial stress experienced by our clients. If our pricing experiences significant downward pressure, our business will be less profitable and our results of operations will be adversely affected. We cannot be certain that we will be able to retain our current clients or expand our client base in this competitive environment. If we do not retain current clients or expand our client base, or if we have to renegotiate existing contracts, our business, financial condition and results of operations will be harmed. Moreover, we expect that competition will continue to increase as a result of consolidation in both the healthcare information technology and healthcare industries. If one or more of our competitors or potential competitors were to merge or partner with another of our competitors, the change in the competitive landscape could also adversely affect our ability to compete effectively and could harm our business, financial condition and results of operations. We have experienced net losses in the past and we may not achieve profitability in the future. We have incurred significant operating losses since our inception. For the years ended January 31, 2023-2024 and January 31, 2022-2023, we had net losses of \$ 136.9 million and \$ 176.1 million and \$ 118.2 million, respectively, and losses from operations of \$ 136.5 million and \$ 176.6 million and \$ 116.8 million, respectively. Our operating expenses may increase in the foreseeable future as we continue to invest to grow our business and build relationships with our clients and partners, develop the Phreesia Platform, develop new solutions and operate as a public company. In addition, to the extent we are successful in increasing our client base, we could incur increased losses because significant costs associated with entering into client agreements are generally incurred up front, while revenue is generally recognized ratably over the term of the agreement. As a result, we may need to raise additional capital through equity and debt financings in order to fund our operations, which may not be available to us on favorable terms or at all. If we are unable to effectively manage these risks and difficulties as we encounter them or effectively access the capital markets, our business, financial condition and results of operations may suffer. Our operating results have in the past and may continue to fluctuate significantly and if we fail to meet the expectations of analysts or investors, our stock price and the value of your investment could decline substantially. Our operating results are likely to fluctuate, and if we fail to meet or exceed the expectations of securities analysts or investors, the trading price of our common stock could decline. Moreover, our stock price may be based on expectations of our future performance that may be unrealistic or that may not be met. Some of the important factors that could cause our revenues and operating results to fluctuate from quarter to quarter include: • the extent to which our products and services achieve or maintain market acceptance; • our ability to introduce new products and services and enhancements to our existing products and services on a timely basis; • new competitors and the introduction of enhanced products and services from new or existing competitors; • the length of our contracting and implementation cycles; • the financial condition of our current and potential clients; • our ability to integrate our Platform solutions with the systems utilized by our healthcare services clients, including but not limited to, EHR and PM systems; • changes in client budgets and procurement policies; • patients' desires to receive communications from Phreesia and / or our partners, and the extent to which they opt- in to such communications, and our ability to deliver a consistent volume of such communications; • amount and timing of our investment in research and development activities and other areas of our business; • technical difficulties or interruptions in our services; • our ability to hire and retain qualified personnel, including the rate of expansion of our sales force; • changes in the regulatory environment related to healthcare; • regulatory compliance costs; • the timing, size and integration success of recent and potential future acquisitions; • unforeseen legal expenses, including litigation and settlement costs; and • buying patterns of our clients and the related seasonality impacts on our business. Many of these factors are not within our control, and the occurrence of one or more of them might cause our operating results to vary widely. As such, we believe that quarter- to- quarter comparisons of our revenues and operating results may not be meaningful and should not be relied upon as an indication of future performance. A significant portion of our operating expense is relatively fixed in nature, and planned expenditures are based in part on expectations regarding future revenue. Accordingly, unexpected revenue shortfalls may decrease our margins and could cause significant changes in our operating results from quarter to quarter. Privacy concerns or security breaches or incidents relating to our Platform SaaS-based solutions could result in economic loss, damage to our reputation, deterring users from using our products, and our exposure to legal penalties and liability. We collect, process and store significant amounts of sensitive, confidential and proprietary information, including personally identifiable information, such as payment data and protected health information,

of patients received in connection with the utilization of our **Platform solutions**. Attacks on information technology systems are increasing in their frequency, levels of persistence, sophistication and intensity, and they are being conducted by increasingly sophisticated and organized groups and individuals with a wide range of motives and expertise, **and they may remain undetected for an extended period of time. If such an event were to occur and cause interruptions in our operations, result in the unauthorized access to, disclosure, loss, processing or other compromise of, personal information or individually identifiable health information (violating certain privacy laws such as HIPAA) or confidential information, or jeopardize the confidentiality, integrity, or availability of our solutions, it could result in a material disruption to our solutions and our business operations.** In addition to extracting sensitive information, such attacks could include the deployment of harmful malware, ransomware, denial- of- service attacks, social engineering and other means to affect service reliability and threaten the confidentiality, integrity and availability of information. The prevalent use of mobile devices also increases the risk of data security incidents. While we believe we have taken reasonable steps to protect such data, techniques used to gain unauthorized access to data and systems, disable or degrade service, or sabotage systems, are constantly evolving, and we may be unable to anticipate such techniques or implement adequate preventative measures to avoid unauthorized access or other adverse impacts to such data or our systems. In addition, some of our third- party service providers and partners also collect and / or store our sensitive information and our clients' data on our behalf, and these service providers and partners are subject to similar threats of cyber -attacks and other malicious internet- based activities, which could also expose us to risk of loss, litigation, and potential liability. **Even though we may have contractual protections with such vendors, contractors, or other organizations, notifications and follow- up actions related to a cybersecurity breach could impact our reputation, cause us to incur significant costs, including legal expenses, harm customer confidence, expose us to government enforcement action, hurt our expansion into new markets, cause us to incur remediation costs, or cause us to lose existing customers.** The risk of state- supported and geopolitical- related cyber- attacks may increase in connection with the war in Ukraine and any related political or economic responses and counter- responses. We may not discover all such incidents or activity or be able to respond or otherwise address them promptly, in sufficient respects or at all. We may be subject to state laws requiring notification of affected individuals and state regulators in the event of a breach of personal information, which is a broader class of information than the health information protected by HIPAA **(as defined below)**. Furthermore, certain health privacy laws, data breach notification laws, consumer protection laws and genetic testing laws may apply directly to our business and / or those of our collaborators and may impose restrictions on our collection, use and dissemination of individuals' health information. Patients about whom we obtain health information, as well as the healthcare services clients who share this information with us, may have statutory or contractual rights that limit our ability to use and disclose the information. We may be required to expend significant capital and other resources to ensure ongoing compliance with applicable privacy and data security laws. Claims that we have violated individuals' privacy rights, violated applicable privacy laws and regulations or breached our contractual obligations, even if we are not found liable, could be expensive and time- consuming to defend and could result in adverse publicity that could harm our business. Like all internet services, our service is vulnerable to software bugs, computer viruses, internet worms, break- ins, phishing attacks, attempts to overload servers with denial- of- service, or other attacks or similar disruptions from unauthorized use of our and third- party computer systems, any of which could lead to system interruptions, delays, or shutdowns, causing loss of critical data or the unauthorized access of data. Though it is difficult to determine what, if any, harm may directly result from any specific interruption or attack, any failure to maintain performance, reliability, security and availability of our products, or failure to prevent software bugs, to the satisfaction of our clients or the health and safety of their patients, such events may harm our reputation and our ability to retain existing clients, and negatively affect our clients and their patients. We have in place systems and processes that are designed to protect our data, prevent data loss, disable undesirable accounts and activities on our **Platform platform** and prevent or detect security breaches, however, we cannot assure you that such measures will provide absolute security. Further, the security systems in place at our employees' and service providers' offices and homes may be less secure than those used in our offices, and while we have implemented technical and administrative safeguards to help protect our systems as our employees and service providers work from their offices, homes and other remote locations, we may be subject to increased cybersecurity risk, which could expose us to risks of data or financial loss, and could disrupt our business operations. There is no guarantee that the data security and privacy safeguards we have put in place will be completely effective or that we will not encounter risks associated with employees and service providers accessing company data and systems remotely. If an actual or perceived breach of security occurs to our systems or a third- party' s systems, we also could be required to expend significant resources to mitigate the breach of security, pay any applicable fines and address matters related to any such breach, including notifying users or regulators, and address reputational harm. Business or economic disruptions or global health concerns could harm our business and increase our costs and expenses. Broad- based business or economic disruptions or global health concerns, ~~such as the COVID-19 pandemic and recent high inflationary environment,~~ could materially and adversely impact our business and results of operations due to, among other factors: • a general decline in business activity, ~~including the impact of our clients' office closures earlier in the COVID-19 pandemic;~~ • a potentially disproportionate impact on the healthcare services clients with whom we contract; • disruptions to our supply chains and our third- party vendors, partners, and suppliers; • difficulty accessing the capital and credit markets on favorable terms, or at all, and a severe disruption and instability in the global financial markets, or deteriorations in credit and financing conditions that could affect our access to capital necessary to fund business operations or address maturing liabilities on a timely basis; and • social, economic, and labor instability in the countries in which we or the third parties with whom we engage operate. In addition, **recent macroeconomic challenges (including high levels of inflation and high interest rates) and the tight labor market volatility continue to adversely affect workforces, the high inflationary environment and organizations, governments, clients, economic economies uncertainty remain widespread, and financial markets globally and have disrupted the normal operations of many businesses, including our business,** making it potentially very difficult

for our clients and us to accurately forecast and plan future business activities. **These factors have and could further decrease healthcare industry spending, adversely affect demand for our products and services, impair the ability of our clients to pay for the products and services they have already purchased from us, cause one or more of our clients to file for bankruptcy protection or go out of business, cause one or more of our clients to fail to renew, terminate, or renegotiate their contracts, impact expected spending from new clients, negatively impact collections of accounts receivable, and harm our business, results of operations, and financial condition. Further, market volatility as a result of future failures of financial institutions, similar to the failures of Silicon Valley Bank and Signature Bank, could lead to market-wide liquidity shortages, impair the ability of companies to access near-term working capital needs and create additional market and economic uncertainty.** During challenging economic times, our clients and patients may have difficulty gaining timely access to sufficient credit or obtaining credit on reasonable terms and may face increased costs or other negative financial impacts, each of which could impair their ability to make timely payments to us and adversely affect our revenue, **which could harm**. ~~If that were to occur~~ **our business, our financial condition and results could be harmed. Further, challenging economic conditions may impair the ability of operations** ~~our clients to pay for the applications and services they already have purchased from us and, as a result, our write-offs of accounts receivable could increase.~~ We are a fully remote company that does not maintain a physical office presence, which subjects us to unique operational risks. Being a fully remote company subjects us to unique operational risks. For example, technologies in our employees' homes may not be as robust as in our offices and could cause the networks, information systems, applications, and other tools available to employees and service providers to be more limited or less reliable than in our offices. Further, the security systems in place at our employees' homes may be less secure than those used in our offices, and while we have implemented technical and administrative safeguards to help protect our systems as our employees and service providers work from home, we may be subject to increased cybersecurity risk, which could expose us to risks of data or financial loss and could disrupt our business operations. There is no guarantee that the data security and privacy safeguards we have put in place will be completely effective or that we will not encounter risks associated with employees accessing company data and systems remotely. In addition, operating remotely may negatively impact our corporate culture, including employee engagement and productivity. If our internal controls over financial reporting or our disclosure controls and procedures are not effective, we may not be able to accurately report our financial results, prevent fraud or file our periodic reports in a timely manner, which may cause investors to lose confidence in our reported financial information and may lead to a decline in our stock price. As a public company, we are required to maintain internal control over financial reporting and disclosure controls and procedures. Section 404 of the Sarbanes-Oxley Act of 2002 (the "Sarbanes-Oxley Act") requires that we evaluate and determine the effectiveness of our internal control over financial reporting and provide a management report on the internal control over financial reporting. Our testing, or the subsequent testing by our independent public accounting firm, may reveal deficiencies in our internal control over financial reporting that are deemed to be material weaknesses. If we are not able to comply with the requirements of Section 404 in a timely manner, or if we or our accounting firm identify deficiencies in our internal control over financial reporting that are deemed to be material weaknesses, the market price of our stock would likely decline and we could be subject to lawsuits, sanctions or investigations by regulatory authorities, including SEC enforcement actions, and we could be required to restate our financial results, any of which would require additional financial and management resources. If material weaknesses in our internal control over financial reporting are discovered or occur in the future, our consolidated financial statements may contain material misstatements and we could be required to restate our financial results, which could materially and adversely affect our business, results of operations and financial condition, restrict our ability to access the capital markets, require us to expend significant resources to correct the material weakness, subject us to fines, penalties or judgments, harm our reputation or otherwise cause a decline in investor confidence. We continue to invest in more robust technology and resources to manage those reporting requirements. Implementing the appropriate changes to our internal controls may distract our officers and employees, result in substantial costs and require significant time to complete. Any difficulties or delays in implementing these controls could impact our ability to timely report our financial results. For these reasons, we may encounter difficulties in the timely and accurate reporting of our financial results, which would impact our ability to provide our investors with information in a timely manner. As a result, our investors could lose confidence in our reported financial information, and our stock price could decline. In addition, any such changes do not guarantee that we will be effective in maintaining the adequacy of our internal controls, and any failure to maintain that adequacy could prevent us from accurately reporting our financial results. We typically incur significant upfront costs in our client relationships, and if we are unable to develop or grow these relationships over time, we are unlikely to recover these costs and our operating results may suffer. We devote significant resources to establish relationships with new clients and deepen relationships with existing clients. Our efforts involve educating our clients and patients about the use, technical capabilities and benefits of our products and services. We do not provide access to our **Platform Solutions** and do not charge fees during this initial sales period. For clients that decide to enter into a contract with us, most of these contracts may provide for a preliminary trial period where a subset of healthcare services locations from the client is granted access to our **Platform solutions**. Following any such trial period, we aim to increase the number of healthcare services locations within the client that utilize our **Platform solutions**. Accordingly, our operating results depend in substantial part on our ability to deliver a successful client and patient experience and persuade our clients and patients to grow their relationship with us over time. As we expect to grow rapidly, our client acquisition costs could outpace revenue growth, and we may be unable to reduce our total operating costs through economies of scale such that we are unable to achieve profitability. Any increased or unexpected costs or unanticipated delays, including delays caused by factors outside of our control, could cause our operating results to suffer. As a result of our variable sales and implementation cycles, we may be unable to recognize revenue to offset expenditures, which could result in fluctuations in our quarterly results of operations or otherwise harm our future operating results. The sales cycle for our services can be variable, typically ranging from three to six months from initial contact to contract execution. During the

sales cycle, we expend time and resources, and we do not recognize any revenue to offset such expenditures. Our implementation cycle is also variable, typically ranging from one to 24 months from contract execution to completion of implementation. The variability of our sales and implementation cycle is dependent on numerous factors, including the discretionary nature of potential clients' purchasing and budget decisions and the size and complexity of the applicable client. Some of our new-client set-up projects are complex and require a lengthy delay and significant implementation work, including to educate prospective clients about the uses and benefits of our **Platform solutions**. Each customer's situation is different, and unanticipated difficulties and delays may arise as a result of failure by us or by the client to meet our respective implementation responsibilities. During the implementation cycle, we expend substantial time, effort and financial resources implementing our service, but accounting principles do not allow us to recognize the resulting revenue until the service has been implemented, at which time we begin recognition of subscription and related implementation revenue over the life of the contract. This could harm our future operating results. If implementation periods are extended, our revenue cycle will be delayed and our financial condition may be adversely affected. In addition, cancellation of any implementation after it has begun may involve loss to us of time, effort and expenses invested in the cancelled implementation process and lost opportunity for implementing paying clients in that same period of time. These factors may contribute to substantial fluctuations in our quarterly operating results, particularly in the near term and during any period in which our sales volume is relatively low. As a result, in future quarters our operating results could fall below the expectations of securities analysts or investors, in which event our stock price would likely decrease. The growth of our business relies, in part, on the growth and success of our clients and certain revenues from our engagements, which is difficult to predict and is subject to factors outside of our control. We enter into agreements with our healthcare services clients, under which a significant portion of our fees are variable, including fees which are dependent upon the number of add-on features ~~to the Phreesia Platform~~ subscribed for by our clients and the number of patients utilizing our payment processing tools. If there is a general reduction in spending by healthcare services organizations on healthcare technology solutions, it may result in a reduction in fees generated from our healthcare services clients or a reduction in the number of add-on features subscribed for by our healthcare services clients. This could lead to a decrease in our revenue, which could harm our business, financial condition and results of operations. In addition, the number of patients utilizing our payment processing tools, and the amounts those patients pay directly to our healthcare services clients for services, is often impacted by factors outside of our control, such as the number of patients with high deductible health plans. Accordingly, revenue under these agreements can be uncertain and unpredictable. If the number of patients utilizing our payment systems, or the aggregate amounts paid by such patients directly to our healthcare services clients through **our solutions** ~~the Phreesia Platform~~, were to be reduced by a material amount, such decrease would lead to a decrease in our revenue, which could harm our business, financial condition and results of operations. We also generate ~~network~~ **Network** solutions revenue through fees charged to our life sciences and payer clients by delivering direct communications to help activate, engage and educate patients who authorize the delivery of, or "opt-in" to, such communications about topics critical to their health. The growth of our revenue stream from life sciences and payer clients is driven, in part, by our ability to grow our network of healthcare services clients and available population of patients to engage, our ability to achieve adequate patient opt-in rates, the number of newly approved drugs and the success of newly launched drugs, each of which is impacted by factors outside of our control. If there is a reduction in newly approved drugs, or newly launched drugs are not successful, this could negatively affect the ability of our life sciences clients to deliver relevant messages to patients who would have otherwise been candidates to receive such drugs, and accordingly may reduce patient opt-in rates. A reduction in the available population of patients to engage or a decline in patient opt-in rates **or a lack of relevant content** could lead to a decrease in our ~~network~~ **Network** solutions revenue, which could harm our business, financial condition and results of operations. If our existing clients are not satisfied with our services, it could have a material adverse effect on our business, financial condition, results of operations and reputation. We depend on our existing clients' satisfaction with our products and services. We expect to derive a significant portion of our revenue from renewal of existing clients' contracts and sales of additional applications and services to existing clients. As part of our growth strategy, we have recently focused on expanding our services amongst current clients. As a result, achieving a high client retention rate, expanding within clients and selling additional applications and services are critical to our future business, revenue growth and results of operations. We also believe that maintaining and enhancing our reputation and brand recognition is critical to our relationships with existing clients and the patients that they serve and to our ability to attract new clients. The promotion of our brand may require us to make substantial investments, and we anticipate that, as our market becomes increasingly competitive, these marketing initiatives may become increasingly difficult and expensive. In addition, the loss or dissatisfaction of any client could substantially harm our brand and reputation, inhibit widespread adoption of **our solutions** ~~the Phreesia Platform~~ and impair our ability to attract new clients. Factors that may affect our client satisfaction and our ability to sell additional applications and services include, but are not limited to, the following: • the price, performance and functionality of our **Platform solutions**; • patient acceptance and adoption of services and utilization of our payment processing tools; • the availability, price, performance and functionality of competing solutions; • our ability to develop and sell complimentary applications and services; • the stability, performance and security of our hosting infrastructure and hosting services; • changes in healthcare laws, regulations or trends; • the business environment of our clients including healthcare staffing shortages and headcount reductions by our clients; and • our ability to maintain and enhance our reputation and brand recognition. We typically enter into annual contracts with our clients, which have a stated initial term of one year and automatically renew for one-year subsequent terms. Most of our clients have no obligation to renew their subscriptions for our ~~Platform solution~~ **solutions** after the initial term expires. In addition, our clients may negotiate terms less advantageous to us upon renewal, which may reduce our revenue from these clients and may decrease our annual revenue. If our clients fail to renew their contracts, renew their contracts upon less favorable terms or at lower fee levels or fail to purchase new products and services from us, our revenue may decline or our future revenue growth may be constrained. Should any of our clients terminate their relationship with us after implementation

has begun, we would not only lose our time, effort and resources invested in that implementation, but we would also have lost the opportunity to leverage those resources to build a relationship with other clients over that same period of time. The estimates and assumptions we use to determine the size of our target market may prove to be inaccurate, and even if the markets in which we compete meet our size estimates and forecasted growth, our business may not grow at similar rates, or at all. Market estimates and growth forecasts that we disclose are subject to significant uncertainty and are based on assumptions and estimates that may not prove to be accurate. The estimates and forecasts relating to the size and expected growth of the market for our services may prove to be inaccurate. These estimates and forecasts may be impacted by economic uncertainty that is outside our control, including international conflicts that may impact international trade and global economic performance and other macroeconomic trends, such as international and domestic supply chain risks, inflationary pressure, interest rate increases and declines in consumer confidence that impact our customers. The principal assumptions relating to our market opportunity include the number of healthcare services organizations currently taking appointments, the amount of annual out of pocket consumer spend for healthcare- related services, and the amount of annual spend by life sciences and payer companies on direct communications with patients at the point of care. Our market opportunity is also based on the assumption that the strategic approach that the Phreesia Platform enables for our potential clients will be more attractive in creating efficiencies in patient care than competing solutions. If these assumptions prove inaccurate, our business, financial condition and results of operations could be adversely affected. If we cannot implement our solutions the Phreesia Platform for clients or resolve any technical issues in a timely manner, we may incur costs in the form of service credits or other remedial steps and / or lose clients, and our reputation may be harmed. Our clients utilize a variety of data formats, applications and infrastructure and we the Phreesia Platform must support our clients' data formats. Furthermore, the healthcare industry has shifted towards digitalized record keeping, and accordingly, many of our healthcare services clients have developed their own software, or utilize third- party software, for practice management and secure storage of electronic medical records. Our ability to develop and maintain logic-based and scalable technology for patient intake management and engagement and payment processing that successfully integrates with our clients' software systems for practice management and storage of electronic medical records is critical. If we do our Platform does not currently support a client' s required data format or appropriately integrate with clients' systems, then we must configure our Platform solutions to do so, which could increase our expenses. Additionally, we do not control our clients' implementation schedules. As a result, if our clients do not allocate the internal resources necessary to meet their implementation responsibilities or if we face unanticipated implementation difficulties, the implementation may be delayed. If the client implementation process is not executed successfully or if execution is delayed, we could incur significant costs, clients could become dissatisfied and decide not to increase utilization of our services the Phreesia Platform or not to implement our solutions the Phreesia Platform beyond an initial period prior to their term commitment or, in some cases, revenue recognition could be delayed. In addition, competitors with more efficient operating models with lower implementation costs could jeopardize our client relationships. Our clients and patients depend on our support services to resolve any technical issues relating to our solutions the Phreesia Platform and our services, and we may be unable to respond quickly enough to accommodate short- term increases in demand for support services, particularly as we increase the size of our client bases (including healthcare services clients and the number of patients that they serve). We also may be unable to modify the format of our support services to compete with changes in support services provided by competitors. It is difficult to predict client and patient demand for technical support services, and if client or patient demand increases significantly, we may be unable to provide satisfactory support services to our clients. Further, if we are unable to address the needs of our clients and their patients in a timely fashion or further develop and enhance our solutions the Phreesia Platform, or if a client or patient is not satisfied with the quality of work performed by us or with the technical support services rendered, then we could incur additional costs to address the situation or be required to issue credits or refunds for amounts related to unused services, and our profitability may be impaired and clients' or patients' dissatisfaction with our solutions the Phreesia Platform could damage our ability to expand the number of applications and services purchased by such clients. These clients may not renew their contracts, seek to terminate their relationships with us or renew on less favorable terms. Moreover, negative publicity related to our client and patient relationships, or regarding patient confidentiality and privacy in the context of technology- enabled healthcare, regardless of its accuracy, may further damage our business by affecting our reputation or ability to compete for new business with current and prospective clients. If any of these were to occur, our revenue may decline and our business, financial condition and results of operations could be adversely affected. We historically derive a significant portion of our revenues from our largest clients. Historically, we have relied on a limited number of clients for a substantial portion of our total revenue and accounts receivable. The sudden loss of any of our larger clients, or the renegotiation of any of their contracts on less favorable terms, could adversely affect our operating results. Because we rely on a limited number of clients for a significant portion of our revenues, we depend on the creditworthiness of these clients. If the financial condition of our larger clients declines, our credit risk could increase. Should one or more of our significant clients declare bankruptcy, it could adversely affect the collectability of our accounts receivable and affect our bad debt reserves and net income. Consolidation in the healthcare industry could have a material adverse effect on our business, financial condition and results of operations. Many healthcare industry participants are consolidating to create larger and more integrated healthcare delivery systems with greater market power. We expect regulatory and economic conditions to result in additional consolidation in the healthcare industry in the future. As consolidation accelerates, the economies of scale of our clients' organizations may grow. If a client experiences sizable growth following consolidation, it may determine that it no longer needs to rely on us and may reduce its demand for our products and services. In addition, as healthcare services organizations and life sciences companies consolidate to create larger and more integrated healthcare delivery systems with greater market power, these healthcare services organizations may try to use their market power to negotiate fee reductions for our products and services. Finally, consolidation may also result in the acquisition or future development by our healthcare services clients and life sciences clients of products and services that compete with our

products and services. Any of these potential results of consolidation could have a material adverse effect on our business, financial condition and results of operations. We depend on our senior management team and certain key employees, and the loss of one or more of our executive officers or key employees or an inability to attract and retain highly skilled employees could adversely affect our business. Our success depends, in part, on the skills, working relationships and continued services of our founders, Chaim Indig (Chief Executive Officer) and Evan Roberts (Chief Operating Officer), and senior management team and other key personnel. From time to time, there may be changes in our senior management team resulting from the hiring or departure of executives, which could disrupt our business. In addition, our shift to a remote work environment could make it increasingly difficult to manage our business and adequately oversee our employees and business functions, potentially resulting in harm to our company culture, increased employee attrition, and the loss of key personnel. In addition, we must attract, train and retain a significant number of highly skilled employees, including sales and marketing personnel, client support personnel, professional services personnel, software engineers, technical personnel and management personnel, and the availability of such personnel, in particular software engineers, may be constrained. We also believe that our future growth will depend on the continued development of our direct sales force and its ability to obtain new clients and to manage our existing client base. If we are unable to hire and develop sufficient numbers of productive direct sales personnel or if new direct sales personnel are unable to achieve desired productivity levels in a reasonable period of time, sales of our services will suffer and our growth will be impeded. Competition for qualified management and employees in our industry is intense, and identifying and recruiting qualified personnel and training them requires significant time, expense and attention. Many of the companies with which we compete for personnel have greater financial and other resources than we do. While we have entered into offer letters or employment agreements with certain of our executive officers, all of our employees are “ at- will ” employees, and their employment can be terminated by us or them at any time, for any reason and without notice, subject, in certain cases, to severance payment rights. The departure and replacement of one or more of our executive officers or other key employees would likely involve significant time and costs, may significantly delay or prevent the achievement of our business objectives and could materially harm our business. In addition, volatility or lack of performance in our stock price may affect our ability to attract replacement should key personnel depart. We **have made, and may in the future** make **future**, acquisitions and investments which may be difficult to integrate, divert management resources, result in unanticipated costs or dilute our stockholders. We have in the past acquired, and we may **continue to in the future** acquire or invest in, businesses, products or technologies that we believe could complement or expand our products and services, enhance our **market coverage or** technical capabilities or otherwise offer growth opportunities . **This may include acquiring or investing in companies, businesses, products or technologies that are tangential to our current business and / or in which we have limited or no prior operating experience** . There are inherent risks in integrating and managing acquisitions, and the pursuit of potential acquisitions may divert the attention of management and cause us to incur various expenses related to identifying, investigating and pursuing suitable acquisitions, whether or not they are consummated. We cannot assure you that we will realize the anticipated benefits of these or any future acquisitions. We also may not achieve the anticipated benefits from the acquired business due to a number of factors, including, without limitation: • difficulty integrating the purchased operations, products or technologies and maintaining the quality and security standards consistent with our brand; • the need to integrate or implement additional controls, procedures and policies; • unanticipated costs or liabilities associated with the acquisition; • our inability to comply with the regulatory requirements applicable to the acquired business; • assimilation of the acquired businesses, which may divert significant management attention and financial resources from our other operations and could disrupt our ongoing business; • use of substantial portions of our available cash **or entail the issuance of our equity securities** or the incurrence of debt to consummate the acquisition; • the loss of key employees, particularly those of the acquired operations; • difficulty retaining or developing the acquired business’ customers; • adverse effects on our existing business relationships; • failure to realize the potential cost savings or other financial benefits or the strategic benefits of the acquisitions, including failure to consummate any proposed or contemplated transaction; and • liabilities from the acquired businesses for infringement of intellectual property rights or other claims and failure to obtain indemnification for such liabilities or claims. Acquisitions also increase the risk of unforeseen legal liability, including for potential violations of applicable law or industry rules and regulations, arising from prior or ongoing acts or omissions by the acquired businesses which are not discovered by due diligence during the acquisition process. Acquisitions could also result in dilutive issuances of equity securities or the incurrence of debt, which could adversely affect our business, results of operations or financial condition. Even if we are successful in completing and integrating an acquired business, it may not perform as we expect or enhance the value of our business as a whole. Certain of our operating results and financial metrics, including the key metrics included in this report, may be difficult to predict as a result of seasonality. We believe there are significant seasonal factors that may cause us to record higher revenue in some quarters compared with others. We believe this variability is largely due to our focus on the healthcare industry. For example, with respect to our healthcare services clients, we receive a disproportionate increase in payment processing revenue from such clients during the first two to three months of the calendar year relative to the other months of the year, which is driven, in part, by the resetting of patient deductibles at the beginning of each calendar year. Sales for our life sciences solutions are also seasonal, primarily due to the annual spending patterns of our clients. This portion of our sales is usually the highest in the fourth quarter of each calendar year. While we believe we have visibility into the seasonality of our business, our rapid growth rate over the last several years may have made seasonal fluctuations more difficult to detect. If our rate of growth slows over time, seasonal or cyclical variations in our operations may become more pronounced, and our business, results of operations and financial position may be adversely affected. Our risk management policies and procedures may not be fully effective in mitigating our risk exposure in all market environments or against all types of risk. We operate in a rapidly changing industry. Accordingly, our risk management policies and procedures may not be fully effective to identify, monitor and manage all risks our business encounters. If our policies and procedures are not fully effective or we are not successful in identifying and

mitigating all risks to which we are or may be exposed, we may suffer uninsured liability, harm to our reputation or be subject to litigation or regulatory actions that could adversely affect our business, financial condition or results of operations. Our ability to limit our liabilities by contract or through insurance may be ineffective or insufficient to cover our future liabilities. We attempt to limit, by contract, our liability for damages arising from our negligence, errors, mistakes or security breaches. Contractual limitations on liability, however, may not be enforceable or may otherwise not provide sufficient protection to us from liability for damages and we are not always able to negotiate meaningful limitations. We maintain liability insurance coverage, including coverage for cyber security and errors and omissions. It is possible, however, that claims could exceed the amount of our applicable insurance coverage, if any, or that this coverage may not continue to be available on acceptable terms or in sufficient amounts. Even if these claims do not result in liability to us, investigating and defending against them could be expensive and time-consuming and could divert management's attention away from our operations. In addition, negative publicity caused by these events may delay market acceptance of our products and services, any of which could materially and adversely affect our reputation and our business. We may become subject to litigation, which could have a material adverse effect on our business, financial condition and results of operations. We may become subject to litigation in the future. Some of these claims may result in significant defense costs and potentially significant judgments against us, some of which we are not, or cannot be, insured against. We generally intend to defend ourselves vigorously; however, we cannot be certain of the ultimate outcomes of any claims that may arise in the future. Resolution of these types of matters against us may result in our having to pay significant fines, judgments or settlements, which, if uninsured, or if the fines, judgments and settlements exceed insured levels, could adversely impact our earnings and cash flows, thereby having a material adverse effect on our business, financial condition, results of operations, cash flow and per share trading price of our common stock. Certain litigation or the resolution of certain litigation may affect the availability or cost of some of our insurance coverage, which could adversely impact our results of operations and cash flows, expose us to increased risks that would be uninsured and adversely impact our ability to attract directors and officers.

Our operations in India will subject us to additional risks which could have an adverse effect on our business, operating results, and financial condition. We have created a subsidiary in India to perform a number of functions currently performed by outside contractors. We expect to hire a significant number of employees from our outside contractor in India to bring these services in-house. While we believe our planned Indian operations will be advantageous to our business, they may also create risks that we must effectively manage. The continued management of our Indian operations will require significant management attention and financial resources that could adversely affect our operating performance. Wages in India are increasing at a faster rate than those in many countries, including the United States. In addition, with the significant increase in the numbers of foreign businesses that have established operations in India, the competition to attract and retain employees there has increased significantly. As a result, we may be unable to cost-effectively retain our current employee base in India or hire additional new talent. In addition, India has experienced significant inflation, low growth in gross domestic product and shortages of foreign exchange. India also has experienced civil unrest and terrorism and, in the past, has been involved in conflicts with neighboring countries. The occurrence of any of these circumstances could result in disruptions to our India operations, which, if continued for an extended period of time, could have a material adverse effect on our business. Further, conducting business abroad may subject us to increased legal and regulatory compliance and oversight. A failure to comply with applicable laws and regulations could result in regulatory enforcement actions, as well as substantial civil and criminal penalties assessed against us and our employees. Our operating expenses incurred outside the United States and denominated in foreign currencies will increase as we expand our operations in India. Transactions denominated in foreign currencies are subject to fluctuations due to changes in foreign currency exchange rates. If we are not able to successfully hedge against the risks associated with foreign currency fluctuations, our financial condition and operating results could be adversely affected.

Risks relating to our payments business If our payments platform is limited, restricted, curtailed or degraded in any way, or if we fail to continue to grow and develop our payments platform, our business may be materially and adversely affected. Our payments platform is a core element of our business. For the fiscal year ended January 31, ~~2023~~ **2024**, our payments platform generated ~~28~~ **27** % of our total revenue. Our future success depends in part on the continued growth and development of our payments platform. If such activities are limited, restricted, curtailed or degraded in any way, or if we fail to continue to grow and develop our payments platform, our business may be materially and adversely affected. The utilization of our payment processing tools may be impacted by factors outside of our control, such as disruptions in the payment processing industry generally. If the number of patients utilizing our payments platform, or the aggregate amounts paid by such patients directly to our healthcare services clients through our payments platform, were to be reduced as a result of disruptions in the payment processing industry or other factors, it could result in a decrease to our revenue, which could harm our business, financial condition and results of operations. In addition, some potential or existing clients may not desire to use our payment processing services or to switch from their existing payment processing vendors for a variety of reasons, such as transition costs, business disruption, and loss of accustomed functionality. There can be no assurance that our efforts to overcome these factors will be successful, and this resistance may adversely affect our growth. The attractiveness of our payment processing services may also depend on our ability to integrate emerging payment technologies, including crypto-currencies, other emerging or alternative payment methods, and credit card systems that we or our processing partners may not adequately support or for which we or they do not provide adequate processing rates. In the event such methods become popular among consumers, any failure to timely integrate emerging payment methods (such as ApplePay) into our software, anticipate client behavior changes, or contract with payment processing partners that support such emerging payment technologies could reduce the attractiveness of our payment processing services, potentially resulting in a corresponding loss of revenue. Increases in card network fees and other changes to fee arrangements may result in the loss of clients who use our payment processing services or a reduction in our earnings. From time to time, card networks, including Visa, MasterCard, American Express and Discover, increase the fees that

they charge acquirers, which would be passed down to processors, payment facilitators and merchants. We could attempt to pass these increases along to our clients, but this strategy might result in the loss of clients to competitors who do not pass along the increases. If competitive practices prevent us from passing along the higher fees to our clients in the future, we may have to absorb all or a portion of such increases, which may increase our operating costs and reduce our earnings. If we fail to comply with the applicable requirements of card networks, they could seek to fine us, suspend us or terminate our payment facilitator status. If our clients or sales partners incur fines or penalties that we cannot collect from them, we may have to bear the cost of such fines or penalties. We provide a payments solution for the secure processing of patient payments. Our payment processing tools can connect to multiple clearinghouses and can also connect directly with patients. We have developed partnerships with primary credit card processors in the United States to facilitate payment processing, and we are registered with Visa, MasterCard, American Express, Discover and other card networks as a service provider (payment facilitator or the equivalent) for acquiring member institutions. These card networks set the operating rules and standards with which we must comply. The termination of our status as a certified service provider, a decision by the card networks to disallow payment facilitators or bar us from serving as such, or any changes in network rules or standards, including interpretation and implementation of the operating rules or standards, that increase the cost of doing business or limit our ability to provide transaction processing services to our clients or partners, could adversely affect our business, financial condition or results of operations. We and our clients are subject to card network rules that could subject us or our clients to a variety of fines or penalties that may be levied by card networks for certain acts or omissions by us or our clients. If a client or sales partner fails to comply with the applicable requirements of card networks, we could be subject to a variety of fines or penalties that may be levied by card networks. We may have to bear the cost of such fines or penalties if we cannot collect them from the applicable client or sales partner, resulting in lower earnings or losses for us. Our violation of the network rules may result in the termination or suspension of our registration with the affected network. The termination of our registration, including a card network barring us from acting as a payment facilitator, or any changes in card network rules that would impair our registration, could require us to stop providing payment processing services relating to the affected card network, which would adversely affect our ability to conduct our business. In addition, the rules of card networks are set by their boards, which may be influenced by card issuers. Many banks directly or indirectly sell processing services to clients in competition with us. These banks could attempt, by virtue of their influence on the networks, to alter the networks' rules or policies to the detriment of non-members, including us. Changes in laws and regulations relating to interchange fees on payment card transactions would adversely affect our revenue and results of operations. We pay interchange fees to the card networks or the card issuers for each transaction we process. The card networks may increase, from time to time, the fees that they charge members or service providers. Although we may attempt to pass these increases along to our clients, this may result in the loss of clients to our competitors that do not pass along the increases. A provision of the Dodd- Frank Wall Street Reform and Consumer Protection Act (the "Dodd- Frank Act") known as the Durbin Amendment empowered the **Board of Governors of the Federal Reserve Board System**, ("FRB-FRS"), to establish and regulate a cap on the interchange fees that **merchants pay issuers (e. g., banks) may charge or receive** for electronic clearing of debit card transactions. The **final rule original regulations** implementing the Durbin Amendment established standards for assessing whether debit card interchange fees received by debit card issuers were reasonable and proportional to the costs incurred by issuers for electronic debit transactions, and it established a maximum permissible interchange fee that an issuer may receive for an electronic debit transaction, limiting the fee revenue to debit card issuers and payment processors. **In November 2023, the FRS proposed amendments to Regulation II that would, if adopted as proposed, significantly lower the maximum permissible interchange fee for such transactions, and such maximum would be reevaluated every two years.** To the extent that HSA- linked payment cards and other exempt payment cards **used on our Platform** (or their issuing banks, **such as those having assets of less than \$ 10 billion**) lose their exempt status under the current rules, **or if any the current** interchange rate caps applicable to **the debit card, credit card or** other payment cards **used on our Platform** are **increased changed**, any such amendment, rule -making, or legislation could impact interchange rates applicable to payment card transactions processed through our **payments Platform platform**. As a result, this could decrease our revenue and profit and could have a material adverse effect on our financial condition and results of operations. Risk relating to our data and intellectual property If our intellectual property is not adequately protected, we may not be able to build name recognition, protect our technology and products, and our business may be adversely affected. Our business depends on proprietary technology and content, including software, databases, confidential information and know- how, the protection of which is crucial to the success of our business. We rely on a combination of trademark, trade- secret and copyright laws, confidentiality procedures and contractual provisions to protect our intellectual property rights in our proprietary technology, content and brand. We may, over time, increase our investment in protecting our intellectual property through additional trademark, patent and other intellectual property filings that could be expensive and time- consuming. Effective trademark, trade- secret and copyright protection is expensive to develop and maintain, both in terms of initial and ongoing registration requirements and the costs of defending our rights. These measures, however, may not be sufficient to offer us meaningful protection. If we are unable to protect our intellectual property and other proprietary rights, our brand, competitive position and business could be harmed, as third parties may be able to dilute our brand or commercialize and use technologies and software products that are substantially the same as ours without incurring the development and licensing costs that we have incurred. Any of our owned or licensed intellectual property rights could be challenged, invalidated, circumvented, infringed or misappropriated, our trade secrets and other confidential information could be disclosed in an unauthorized manner to third parties, or our intellectual property rights may not be sufficient to permit us to take advantage of current market trends or otherwise provide us with competitive advantages, which could result in costly redesign efforts, discontinuance of certain offerings or other competitive harm. Monitoring unauthorized use of our intellectual property is difficult and costly. From time to time, we seek to analyze our competitors' products and services, and may in the future seek to enforce our rights against potential infringement. However, the

steps we have taken to protect our proprietary rights may not be adequate to prevent infringement or misappropriation of our intellectual property. We may not be able to detect unauthorized use of, or take appropriate steps to enforce, our intellectual property rights. Any inability to meaningfully protect our intellectual property rights could result in harm to our brand or our ability to compete and reduce demand for our technology and products. Moreover, our failure to develop and properly manage new intellectual property could adversely affect our market positions and business opportunities. Also, some of our products and services rely on technologies and software developed by or licensed from third parties. Any disruption or disturbance in such third- party products or services, which we have experienced in the past, could interrupt the operation of our **Platform solutions**. We may not be able to maintain our relationships with such third parties or enter into similar relationships in the future on reasonable terms or at all. We may also be required to protect our proprietary technology and content in an increasing number of jurisdictions, a process that is expensive and may not be successful, or which we may not pursue in every location. In addition, effective intellectual property protection may not be available to us in every country, and the laws of some foreign countries may not be as protective of intellectual property rights as those in the United States. Additional uncertainty may result from changes to intellectual property legislation enacted in the United States and elsewhere, and from interpretations of intellectual property laws by applicable courts and agencies. Accordingly, despite our efforts, we may be unable to obtain and maintain the intellectual property rights necessary to provide us with a competitive advantage. Our failure to obtain, maintain and enforce our intellectual property rights could therefore have a material adverse effect on our business, financial condition and results of operations. Our use of “ open source ” software could adversely affect our ability to offer our services and subject us to possible litigation. We may use open source software in connection with our products and services. Companies that incorporate open source software into their products have, from time to time, faced claims challenging the use of open source software and / or compliance with open source license terms. As a result, we could be subject to suits by parties claiming ownership of what we believe to be open source software or claiming noncompliance with open source licensing terms. Some open source software licenses require users who distribute software containing open source software to publicly disclose all or part of the source code to such software and / or make available any derivative works of the open source code, which could include valuable proprietary code of the user, on unfavorable terms or at no cost. While we monitor the use of open source software and try to ensure that none is used in a manner that would require us to disclose our proprietary source code or that would otherwise breach the terms of an open source agreement, such use could inadvertently occur, in part because open source license terms are often ambiguous. Any requirement to disclose our proprietary source code or pay damages for breach of contract could have a material adverse effect on our business, financial condition and results of operations and could help our competitors develop products and services that are similar to or better than ours. Any restrictions on our use of, or ability to license, data, or our failure to license data and integrate third- party technologies, could have a material adverse effect on our business, financial condition and results of operations. We depend upon licenses from third parties for some of the technology and data used in our applications, and for some of the technology platforms upon which these applications are built and operate. We expect that we may need to obtain additional licenses from third parties in the future in connection with the development of our products and services. In addition, we obtain a portion of the data that we use from government entities, public records and our partners for specific partner engagements. We believe that we have all rights necessary to use the data that is incorporated into our products and services. However, we cannot assure you that our licenses for information will allow us to use that information for all potential or contemplated applications and products. In addition, our ability to use data to support existing products and services and to develop new products and services is largely dependent upon the contractual rights we secure. For example, certain of our products depend on maintaining our data and analytics platform, which is populated with data disclosed to us by healthcare services clients, life sciences companies and their respective patients and other partners with their consent. If these clients, patients or partners revoke their consent for us to maintain, use, de- identify and share this data, consistent with applicable law, our data assets could be degraded. In the future, data providers could withdraw their data from us or restrict our usage for any reason, including if there is a competitive reason to do so, if legislation is passed restricting the use of the data or if judicial interpretations are issued restricting use of the data that we currently use in our products and services. In addition, data providers could fail to adhere to our quality control standards in the future, causing us to incur additional expense to appropriately utilize the data. If a substantial number of data providers were to withdraw or restrict their data, or if they fail to adhere to our quality control standards, and if we are unable to identify and contract with suitable alternative data suppliers and integrate these data sources into our service offerings, our ability to provide products and services to our partners would be materially adversely impacted, which could have a material adverse effect on our business, financial condition and results of operations. We also integrate into our proprietary applications and use third- party software to maintain and enhance, among other things, content generation and delivery, and to support our technology infrastructure. Some of this software is proprietary and some is open source software. Our use of third- party technologies and open source software exposes us to increased risks, including, but not limited to, risks associated with the integration of new technology into **our solutions** the Phreesia Platform, the diversion of our resources from development of our own proprietary technology and our inability to generate revenue from licensed technology sufficient to offset associated acquisition and maintenance costs. These technologies may not be available to us in the future on commercially reasonable terms or at all and could be difficult to replace once integrated into our own proprietary applications. Most of these licenses can be renewed only by mutual consent and may be terminated if we breach the terms of the license and fail to cure the breach within a specified period of time. Our inability to obtain, maintain or comply with any of these licenses could delay development until equivalent technology can be identified, licensed and integrated, which would harm our business, financial condition and results of operations. Most of our third- party licenses are non- exclusive and our competitors may obtain the right to use any of the technology covered by these licenses to compete directly with us. If our data suppliers choose to discontinue support of the licensed technology in the future, we might not be able to modify or adapt our own solutions. Third parties may initiate legal proceedings alleging that we are infringing or otherwise violating their intellectual property rights, the

outcome of which would be uncertain and could have a material adverse effect on our business, financial condition and results of operations. Our commercial success depends on our ability to develop and commercialize our services and use our proprietary technology without infringing the intellectual property or proprietary rights of third parties. Intellectual property disputes can be costly to defend and may cause our business, operating results and financial condition to suffer. As the market for healthcare in the United States expands and more patents are issued, the risk increases that there may be patents issued to third parties that relate to our products and technology of which we are not aware or that we must challenge to continue our operations as currently contemplated. Whether merited or not, we may face allegations that we, our partners, our licensees or parties indemnified by us have infringed or otherwise violated the patents, trademarks, copyrights or other intellectual property rights of third parties. Such claims may be made by competitors seeking to obtain a competitive advantage or by other parties. Additionally, in recent years, individuals and groups have begun purchasing intellectual property assets for the purpose of making claims of infringement and attempting to extract settlements from companies like ours. We may also face allegations that our employees have misappropriated the intellectual property or proprietary rights of their former employers or other third parties. It may be necessary for us to initiate litigation to defend ourselves in order to determine the scope, enforceability and validity of third- party intellectual property or proprietary rights, or to establish our respective rights. Regardless of whether claims that we are infringing patents or other intellectual property rights have merit, such claims can be time- consuming, divert management' s attention and financial resources and can be costly to evaluate and defend. Results of any such litigation are difficult to predict and may require us to stop commercializing or using our products or technology, obtain licenses, modify our services and technology while we develop non- infringing substitutes or incur substantial damages, settlement costs or face a temporary or permanent injunction prohibiting us from marketing or providing the affected products and services. If we require a third- party license, it may not be available on reasonable terms or at all, and we may have to pay substantial royalties, upfront fees or grant cross- licenses to intellectual property rights for our products and services. We may also have to redesign our products or services so they do not infringe third- party intellectual property rights, which may not be possible or may require substantial monetary expenditures and time, during which our technology and products may not be available for commercialization or use. Even if we have an agreement to indemnify us against such costs, the indemnifying party may be unable to uphold its contractual obligations. If we cannot or do not obtain a third- party license to the infringed technology, license the technology on reasonable terms or obtain similar technology from another source, our revenue and earnings could be adversely impacted. From time to time, we may be subject to legal proceedings and claims in the ordinary course of business with respect to intellectual property. We are not currently subject to any claims from third parties asserting infringement of their intellectual property rights. Some third parties may be able to sustain the costs of complex litigation more effectively than we can because they have substantially greater resources. Even if resolved in our favor, litigation or other legal proceedings relating to intellectual property claims may cause us to incur significant expenses and could distract our technical and management personnel from their normal responsibilities. In addition, there could be public announcements of the results of hearings, motions or other interim proceedings or developments, and if securities analysts or investors perceive these results to be negative, it could have a material adverse effect on the price of our common stock. Moreover, any uncertainties resulting from the initiation and continuation of any legal proceedings could have a material adverse effect on our ability to raise the funds necessary to continue our operations. Assertions by third parties that we violate their intellectual property rights could therefore have a material adverse effect on our business, financial condition and results of operations. Interruption or failure of our information technology and communications systems could impair our ability to effectively deliver our products and services, which could cause us to lose clients and harm our operating results. Our business depends on the continuing operation of our technology infrastructure and systems. Proprietary software development is time- consuming, expensive and complex, and may involve unforeseen difficulties. We may encounter technical obstacles in enhancing our existing software and developing new software, and it is possible that we may discover additional problems that prevent our proprietary applications from operating properly. In addition, any damage to or failure of our existing systems could result in interruptions in our ability to deliver our products and services. Interruptions in our service could reduce our revenue and profits, and our reputation could be damaged if people believe our systems are unreliable. Our systems and operations are vulnerable to damage or interruption from natural disasters or man- made problems, such as earthquakes, floods, fires, political unrest, acts of terrorism, armed conflict or war (such as the current Russian invasion of Ukraine **and the conflict in the Middle East**), power loss, break- ins, hardware or software failures, telecommunications failures, computer viruses or other attempts to harm our systems and similar events. Any unscheduled interruption in our service would result in an immediate loss of revenue. Frequent or persistent system failures that result in the unavailability of our **Platform solutions** or slower response times could reduce our clients' ability to access our **Platform solutions**, impair our delivery of our products and services and harm the perception of our **Platform solutions** as reliable, trustworthy and consistent. Our insurance policies provide only limited coverage for service interruptions and may not adequately compensate us for any losses that may occur due to any failures or interruptions in our systems. If our services fail to provide accurate and timely information, or if our content or any other element of our service is associated with errors or malfunctions, we could have liability to clients or patients which could adversely affect our results of operations. Our software, content and services are used to assist medical groups, health systems and payers with managing the patient intake process and to empower patients and healthcare organizations as they navigate the challenges of an evolving healthcare system. If our software, content or services fail to provide accurate and timely information or are associated with errors or malfunctions, then healthcare services clients or patients could assert claims against us that could result in substantial costs to us, harm our reputation in the industry and cause demand for our services to decline. Our proprietary service is utilized in patient intake and engagement and to help healthcare services organizations better understand patients through medical histories, insurance benefits and socio- economic indicators. If our service fails to provide accurate and timely information, or if our content or any other element of our service is associated with errors or malfunctions, we could have liability to healthcare services clients or

patients. We attempt to limit by contract our liability for damages and to require that our clients assume responsibility for medical care and approve key system rules, protocols and data. Despite these precautions, the allocations of responsibility and limitations of liability set forth in our contracts may not be enforceable, may not be binding upon patients or may not otherwise protect us from liability for damages. Our proprietary software may contain errors or failures that are not detected until after the software is introduced or updates and new versions are released. It is challenging for us to test our software for all potential problems because it is difficult to simulate the wide variety of computing environments or methodologies that our clients may deploy or rely upon. From time to time we have discovered defects or errors in our software, and such defects or errors can be expected to appear in the future. Defects and errors that are not timely detected and remedied could expose us to risk of liability to healthcare services clients and patients and cause delays in introduction of new services, result in increased costs and diversion of development resources, require design modifications or decrease market acceptance or client satisfaction with our services. If any of these risks occur, they could materially adversely affect our business, financial condition or results of operations. We may be liable for use of incorrect or incomplete data we provide which could harm our business, financial condition and results of operations. We collect, store and display data, including patient health information, for use by healthcare services clients in handling patient intake and engagement. Our clients, their patients, or third parties provide us with most of this data. If this data is incorrect or incomplete or if we make mistakes in the capture or input of this data, adverse consequences may occur and give rise to product liability and other claims against us. In addition, a court or government agency may take the position that our storage and display of health information exposes us to liability arising out of our intake, storage and display of erroneous health information. While we maintain insurance coverage, we cannot be certain that this coverage will prove to be adequate or will continue to be available on acceptable terms, if at all. Even unsuccessful claims could result in substantial costs and diversion of management resources. A claim brought against us that is uninsured or under-insured could harm our business, financial condition and results of operations. Risks relating to laws and regulations applicable to our **industry** We are subject to health care laws and data privacy and security laws and regulations governing our collection, use, disclosure, storage and transmission of personally identifiable information, including protected health information and payment card data, which may impose restrictions on us and our operations, require us to change our business practices and put in place additional compliance mechanisms, and subject us to fines, penalties, lawsuits, adverse publicity, reputational harm, loss of customer trust or government enforcement actions if we are unable to fully comply with such laws. Numerous complex federal and state laws and regulations govern the collection, use, disclosure, storage and transmission of personally identifiable information, including protected health information. State laws may be even more restrictive and not preempted by HIPAA, **(as defined below)**, and may be subject to varying interpretations by the courts and government agencies. These laws and regulations, including their interpretation by governmental agencies, are subject to frequent change and could have a negative impact on our business. Further, these varying interpretations could create complex compliance issues for us and our partners and potentially expose us to additional expense, liability, penalties, negatively impact our client relationships, and lead to adverse publicity, and all of these risks could adversely affect our business in the short and long term. In addition, contractual obligations and in the future, legislation may limit, forbid or regulate the use or transmission of health information outside of the United States or across other national borders. These developments, if adopted, could render our use of Canadian employees and other non- U. S. resources for work related to such data impracticable or substantially more expensive. We are a " Business Associate " as defined under the federal Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act (" HITECH Act") and their implementing regulations, collectively referred to as HIPAA. The U. S. Department of Health and Human Services, (" HHS"), Office for Civil Rights, may impose civil penalties on a Business Associate for a failure to comply with HIPAA requirements. The U. S. Department of Justice is responsible for criminal prosecutions under HIPAA. Penalties can vary significantly depending on a number of factors, such as whether the Business Associate's failure to comply was due to willful neglect. State attorneys general also have the right to prosecute HIPAA violations committed against residents of their states. While HIPAA does not create a private right of action that would allow individuals to sue in civil court for HIPAA violations, its standards have been used as the basis for the duty of care in state civil suits, such as those for recklessness in misusing individuals' health information. If we are subject to investigation or litigation related to an alleged violation of HIPAA, then we may elect to resolve the matter through a settlement. Such settlement could require payment of a civil penalty or damages, corrective action and / or monitoring of our business by a third party. The security measures that we and our third- party vendors and subcontractors have in place to ensure compliance with privacy and data protection laws **may are not protect our facilities-guarantees that we and systems from our subcontractors will not be the victims of security-cybersecurity breaches-attacks**, acts of vandalism or theft, computer viruses, misplaced or lost data, malfeasance, programming and human errors or other similar events. Under the HITECH Act, as a Business Associate we may also be liable for privacy and security breaches and failures of our subcontractors. Even though we provide for appropriate protections through our agreements with our subcontractors, we still have limited control over their actions and practices. A breach of privacy or security of individually identifiable health information by a subcontractor may result in an enforcement action, including criminal and civil liability, against us. We are not able to predict the extent of the impact such incidents may have on our business. Our failure to comply may result in criminal and civil liability because the potential for enforcement action against Business Associates is now greater. Enforcement actions against us could be costly and could interrupt regular operations, which may adversely affect our business. While we have not received any notices of violation of the applicable privacy and data protection laws and believe we are in compliance with such laws, there can be no assurance that we will not receive such notices in the future. Even when HIPAA does not apply, according to the Federal Trade Commission, or the FTC, failing to take appropriate steps to keep consumers' personal information secure constitutes unfair acts or practices in or affecting commerce in violation of Section 5 (a) of the Federal Trade Commission Act, or the FTCA, 15 U. S. C. § 45 (a). The FTC expects a company's data security measures to be reasonable and appropriate in light of the sensitivity and

volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. Individually identifiable health information is considered sensitive data that merits stronger safeguards. The FTC's current guidance for appropriately securing consumers' personal information is similar to what is required by the HIPAA security regulations, but this guidance may change in the future, resulting in increased complexity and the need to expend additional resources to ensure we are complying with the FTCA. Other federal and state laws restrict the use and protect the privacy and security of personally identifiable information are, in many cases, are not preempted by HIPAA and may be subject to varying interpretations by the courts and government agencies. These varying interpretations can create complex compliance issues for us and our partners and potentially expose us to additional expense, adverse publicity and liability, any of which could adversely affect our business. Federal and state consumer protection laws are increasingly being applied by the United States Federal Trade Commission and states' attorneys general to regulate the collection, use, storage and disclosure of personal or personally identifiable information, through websites or otherwise, and to regulate the presentation of website content. There is ongoing concern from privacy advocates, regulators and others regarding data privacy and security issues, and the number of jurisdictions with data privacy and security laws has been increasing. Also, there are ongoing public policy discussions regarding whether the standards for de-identification, anonymization or pseudonymization of health information are sufficient, and the risk of re-identification sufficiently small, to adequately protect patient privacy. We expect that there will continue to be new proposed and amended laws, regulations and industry standards concerning privacy, data protection and information security in the United States, such as the CCPA, as amended by the California Privacy Rights Act, or CPRA, which amendments went into effect on January 1, 2023, The CCPA creates specific obligations with respect to processing and storing personal information, and the CPRA amendments created a new state agency that is vested with authority to implement and enforce the CCPA. **Additionally, in addition to the CCPA, new privacy and data security laws have been enacted in numerous states and have been proposed in even more states as well as in the U. S. Congress. If passed, these new laws could impose similar or more restrictive requirements than these recently enacted laws. Furthermore, other states have proposed or enacted legislation that is focused on more narrow aspects of privacy. For example, a similar number of states have passed law laws went into effect in Virginia that protect biometric information and a smaller number of states have passed or are considering laws that are specifically focused upon health privacy, such as Washington's My Health My Data Act. The My Health, My Data Act imposes new state restrictions and requirements on the processing January 1, 2023, and further US-sale of consumer health data and creates a private right of action. The effects of state comprehensive and federal privacy laws are set potentially significant and may require us to go into effect throughout 2023, including laws modify our data processing practices and policies and to incur substantial costs and potential liability in Colorado, Connecticut, and an Utah effort to comply with such legislation.** We cannot yet determine the full impact these laws or other such future laws, regulations and standards may have on our current or future business. Any of these laws may broaden their scope in the future, and similar laws have been proposed on both a federal level and in **various more than half of the states in the U. S. A number of other states have proposed new privacy laws, some of which are similar to the above discussed recently passed laws.** Such proposed legislation, if enacted, may add additional complexity, variation in requirements, restrictions and potential legal risk, require additional investment of resources in compliance programs, impact strategies and the availability of previously useful data and could result in increased compliance costs and / or changes in business practices and policies. The existence of comprehensive privacy laws in different states in the country, **and the heightened scrutiny associated with the enforcement of such laws, would could** make our compliance obligations more complex and costly and may increase the likelihood that we may be subject to enforcement actions or otherwise incur liability for noncompliance. We also expect that there will continue to be new or amended laws, regulations, standards and obligations proposed and enacted in various jurisdictions. Many countries around the world have enacted comprehensive privacy and data protection laws that can impact our business. For example, in May 2018, the General Data Protection Regulation, or GDPR, went into effect in the European Union, or EU. The GDPR imposes more stringent data protection requirements and requires businesses subject to it to give more detailed disclosures about how they collect, use, and share personal information; contractually commit to data protection measures in contracts; maintain adequate data security measures; notify regulators and affected individuals of certain data breaches; obtain consent to collect sensitive personal information such as health information **or ensuring another appropriate legal basis or condition applies to the processing of personal information**; meet extensive privacy governance and documentation requirements; and honor individuals' data protection rights, **including their rights to access, correct, and delete their personal information.** The GDPR also imposes strict rules on the transfer of personal information to countries outside of the European Economic Area, or EEA **to jurisdictions that the European Commission (EC) does not recognize as having "adequate" data protection laws. These transfers are prohibited unless a valid transfer mechanism is implemented, such as the Standard Contractual Clauses (SCCs) published by the EC, including binding corporate rules or certification to the United States. A recent judicial decision from the EU - U. S. Data Privacy Framework that the EC adopted on July 10, 2023. Evolving laws and decisions surrounding recent announcements from European regulators regarding transfers of EU personal information outside of the EEA have increased the legal risks and liabilities, and compliance and operational costs, of lawfully making such transfers. Companies that violate the GDPR can face private litigation, restrictions, or prohibitions on data processing, and fines of up to the greater of 20 million Euros or 4 % of worldwide annual revenue. In addition, further to the UK's exit from the EU on January 31, 2020, the GDPR ceased to apply in the UK at the end of the transition period on December 31, 2020 -; **However however, as of January 1, 2021,** the UK's European Union (Withdrawal) Act 2018 incorporated the GDPR (as it existed on December 31, 2020 but subject to certain UK specific amendments) into UK law, referred to as the UK GDPR. The UK GDPR and the UK Data Protection Act 2018 set out the UK's data protection regime, which is independent from but aligned to the EU's data protection regime. Non-compliance with the UK GDPR may result in monetary penalties of up to £ 17. 5 million or 4 % of worldwide revenue, whichever is higher.**

Although the GDPR and the UK GDPR currently impose substantially similar obligations, it is possible that over time the UK GDPR could become less aligned with the GDPR. The UK government has announced plans to reform the data protection legal framework in the UK in its Data Reform Bill but, **which will introduce significant changes from those that have been put on hold GDPR. This may lead to additional compliance costs and could increase our overall risk exposure as we may no longer be able to take a unified approach across the EEA and the UK.** This lack of clarity on future UK laws and regulations and their interaction with EU laws and regulations could add legal risk, uncertainty, complexity and cost to our handling of EU personal information and our privacy and data security compliance programs and could require us to implement different compliance measures for the UK and the EU. Although the UK is regarded as a third country under the EU's GDPR, the European Commission (the "EC"), has now issued a decision recognizing the UK as providing adequate protection under the EU GDPR and, therefore, transfers of personal data originating in the EU to the UK remain unrestricted. Like the EU GDPR, the UK GDPR restricts personal data transfers outside the UK to countries not regarded by the UK as providing adequate protection. The UK government has confirmed that personal data transfers from the UK to the EEA remain free flowing. To enable the transfer of personal data outside of the EEA or the UK, adequate safeguards must be implemented in compliance with European and UK data protection laws. **On June 4, 2021, such as the EC issued new forms of standard Standard contractual Contractual clauses - Clauses (SCCs) published by the European Commission, binding corporate rules for - or certification to data transfers from controllers or processors in the EU - U / EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU / EEA (and not subject to the GDPR).** **S. Data Privacy Framework** The new standard contractual clauses replace the standard contractual clauses that were **the European Commission** adopted **on July 10, 2023** previously under the EU Data Protection Directive. The UK is not subject to the EC's **SCCs new standard contractual clauses** but has published the UK International Data Transfer Agreement and International Data Transfer Addendum to the new standard contractual clauses (the "IDTA"), which enable transfers from the UK. For new transfers, the IDTA already needs to be in place, and must be in place for all existing transfers from the UK from March 21, 2024. Following a ruling from the Court of Justice of the EU, in Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems, Case C- 311 / 18 (" Schrems II"), companies relying on **SCCs standard contractual clauses** to govern transfers of personal data to third countries (in particular the United States) will need to assess whether the data importer can ensure sufficient guarantees for safeguarding the personal data under GDPR. This assessment includes assessing whether third- party vendors can also ensure these guarantees. The same assessment is required for transfers governed by the IDTA. We will be required to implement these new safeguards when conducting restricted data transfers under the GDPR and doing so will require significant effort and cost. **Moreover On March 25, on September 21, 2022-2023**, the **European Commission and UK Government adopted the Data Protection (Adequacy) Regulations 2023, also referred to as the " UK- U. S. White House announced that an agreement Data Bridge ", which will allow companies to transfer personal data from the UK to the United States on the basis of the EU- U. S. Data Privacy Framework Shield 2.0** **Some 0 has been reached. However, it is too soon to tell how the future of the businesses we Privacy Shield 2.0 will evolve and what impact it will have on our cross- border activities. Insignia Health, LLC, which we acquired are in December 2021, is subject to additional laws and regulations in jurisdictions outside of the United States**, including those in the EEA and UK, such as the GDPR and UK GDPR. Compliance with such laws and regulations requires resources and could be more costly and take more time than we anticipate and could involve new fines or penalties for non- compliance, all of which could adversely affect our business. **The In addition to the GDPR and UK has additional GDPR, the EU e- privacy Privacy Directive (2002 / 58 / EC) and consumer protection laws, such as the UK Privacy and Electronic Communications Regulations 2003 govern**, to which our marketing messages **we send** to **actual or potential customers based in the EEA and UK -based customers may be subject**. We have operations in Canada, where our collection, use, disclosure, and management of personal information must comply with both federal and provincial privacy laws, which impose separate requirements, but may overlap in some instances. The Personal Information Protection and Electronic Documents Act (" PIPEDA") applies in all Canadian provinces except Alberta, British Columbia and Québec, as well as to the transfer of consumer data across provincial borders. PIPEDA imposes stringent consumer data protection obligations, requires privacy breach reporting, and limits the purposes for which organizations may collect, use, and disclose consumer data. The provinces of Alberta, British Columbia, and Québec have enacted separate data privacy laws that are substantially similar to PIPEDA, but all three additionally apply to our handling of our own employees' personal data within their respective provinces. Notably, Québec's Act respecting the protection of personal information in the private sector, or the Private Sector Act, was amended by Bill 64, an Act to modernize legislative provisions as regards the protection of personal information, which introduced major amendments to the Private Sector Act, notably, to impose significant and stringent new obligations on Québec businesses while increasing the powers of Quebec's supervisory authority. We may incur additional costs and expenses related to compliance with these laws and may incur significant liability if we are not able to comply with these laws. We are also subject to Canada's anti- spam legislation, or CASL, which includes rules governing commercial electronic messages, which include marketing emails, text messages, and social media advertisements. Under these rules, we must follow certain standards when sending marketing communications, are prohibited from sending them to customers without their consent, and can be held liable for violations. Internationally, virtually every jurisdiction in which we operate has established its own data security and privacy legal framework with which we or our customers must comply. Cross- border data transfers and other future developments regarding local data residency and access could increase the cost and complexity of delivering our services in some markets and may lead to governmental enforcement actions, litigation, fines, and penalties or adverse publicity, which could adversely affect our business and financial position could greatly increase our cost of providing our products and services, require significant changes to our operations or even prevent us from offering certain services in specific jurisdictions. In addition, any limitation on our ability to use or transmit health information outside of the U. S. could impose restrictions on our ability to recruit and maintain employees residing outside of the U. S., which could, in turn, adversely affect our business.

Future laws, regulations, standards, obligations amendments, and changes in the interpretation of existing laws, regulations, standards and obligations could impair our or our clients' ability to collect, use or disclose information relating to consumers, which could decrease demand for our **Platform solutions**, increase our costs and impair our ability to maintain and grow our client base and increase our revenue. New laws, amendments to or re- interpretations of existing laws and regulations, industry standards and contractual obligations could impair our or our customers' ability to collect, use or disclose information relating to patients or consumers, which could decrease demand for our platform offerings, increase our costs and impair our ability to maintain and grow our client base and increase our revenue. Accordingly, we may find it necessary or desirable to fundamentally change our business activities and practices or to expend significant resources to modify our software ~~or Platform~~ and otherwise adapt to these changes. We are also subject to self- regulatory standards and industry certifications that may legally or contractually apply to us. These include the Payment Card Industry Data Security Standards (" PCI- DSS") and AICPA Security Organization Control 2 (" SOC 2"), with which we are currently compliant, and HITRUST certification, which we currently maintain. In the event we fail to comply with the PCI- DSS or fail to maintain our SOC 2 or HITRUST certification, we could be in breach of our obligations under customer and other contracts, fines and other penalties could result, and we may suffer reputational harm and damage to our business. Further, our clients may expect us to comply with more stringent privacy, data storage and data security requirements than those imposed by laws, regulations or self- regulatory requirements, and we may be obligated contractually to comply with additional or different standards relating to our handling or protection of data. Any failure or perceived failure by us to comply with domestic or foreign laws or regulations, industry standards or other legal obligations, or any actual or suspected privacy or security incident, whether or not resulting in unauthorized access to, or acquisition, release or transfer of personally identifiable information or other data, may result in governmental enforcement actions and prosecutions, private litigation, fines and penalties or adverse publicity and could cause our clients to lose trust in us, which could have an adverse effect on our reputation and business. We may be unable to make such changes and modifications in a commercially reasonable manner or at all, and our ability to develop new products and features could be limited. Any of these developments could harm our business, financial condition and results of operations. Privacy and data security concerns, whether valid or not valid, may inhibit retention of ~~our Platform or~~ services by existing clients or adoption of our ~~Platform or~~ services by new clients. Existing laws regulate our ability to engage in direct marketing and changes in privacy laws could adversely affect our ability to market our products effectively and could impact our results from operations or result in costs and fines. We rely on a variety of direct marketing techniques, including email marketing. These activities are regulated by legislation such as the Controlling the Assault of Non- Solicited Pornography and Marketing (CAN- SPAM) Act of 2003. Any failure by us to comply fully with the CAN- SPAM Act may leave us subject to substantial fines and penalties. In addition, any future restrictions in laws such as the CAN- SPAM Act, and various United States state laws, or new federal laws regarding marketing and solicitation or international data protection laws that govern these activities could adversely affect the continuing effectiveness of our marketing efforts and could force changes in our marketing strategies. If this occurs, we may not be able to develop adequate alternative marketing strategies, which could have a material adverse impact on our results of operations. Any failure by us to comply fully with website accessibility standards could result in us being subject to considerable fines and penalties. We conduct business through various Internet websites and web- based applications that are subject to accessibility requirements. Courts have ruled that the Americans with Disabilities Act (ADA) applies to Internet websites and other digital experiences and litigation related to ADA website accessibility has soared in recent years. Failing to comply with those requirements could leave our Company subject to claims, litigation, lawsuits and, ultimately, substantial fines and penalties. The healthcare regulatory and political framework is uncertain and evolving. Healthcare laws and regulations are rapidly evolving and may change significantly in the future, which could adversely affect our financial condition and results of operations. For example, in ~~March~~ 2010, the Patient Protection and Affordable Care Act (" ACA") was adopted, which is a healthcare reform measure that provides healthcare insurance for millions of Americans. The ACA includes a variety of healthcare reform provisions and requirements that became effective at varying times through 2018 and substantially changes the way healthcare is financed by both governmental and private insurers, which may significantly impact our industry and our business. Since its enactment, there have been numerous judicial, administrative, executive, and legislative challenges to certain aspects of the ACA. It is unclear how other healthcare reform measures of the Biden administration or other efforts, if any, to challenge, repeal or replace the ACA will impact our business. Further, ~~in on March 9,~~ 2020, the HHS, Office of the National Coordinator for Health Information Technology (" ONC") and CMS promulgated final rules aimed at supporting seamless and secure access, exchange, and use of electronic health information (" EHI"), **referred to as the Final Rule**, by increasing innovation and competition by giving patients and their healthcare service providers secure access to health information and new tools, allowing for more choice in care and treatment. The ~~final Final rules Rules are is~~ intended to clarify and operationalize provisions of the 21st Century Cures Act (" Cures Act"), regarding interoperability and " information blocking, " and create significant new requirements for health care industry participants. Information blocking is defined as activity that is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI, where a health information technology developer, health information network or health information exchange knows or should know that such practice is likely to interfere with access to, exchange or use of EHI. **In April 2023, the ONC issued a notice of proposed rulemaking that would modify certain components of the Final Rule, including modifying and expanding certain exceptions to the information blocking regulations, which are intended to support information sharing.** The ~~final Final CMS rule Rule~~ focuses on patients enrolled in Medicare Advantage plans, Medicaid and Children's Health Insurance Program (" CHIP") fee- for- service programs, Medicaid managed care plans, CHIP managed care entities, and qualified health plans on the federally- facilitated exchanges, and enacts measures to enable patients to have both their clinical and administrative information travel with them. Recent regulatory reform constitutes a significant departure from previous regulations regarding patient data. While these rules benefit us in that certain EHR vendors will no longer be permitted to interfere with our attempts at integration, they may also

make it easier for other similar companies to enter the market, creating increased competition and reducing our market share. It is unclear at this time what the costs of compliance with the ~~final~~ **Final rules-Rule** will be, and what additional risks there may be to our business. In addition, we are subject to various other laws and regulations, including, among others, anti-kickback laws, antitrust laws and the privacy and data protection laws described below. We conduct business in a heavily regulated industry, and any failure to comply with applicable healthcare laws and government regulations, could result in financial penalties, exclusion from participation in government healthcare programs and adverse publicity, or could require us to make significant operational changes, any of which could harm our business. Our current and future arrangements with healthcare professionals, principal investigators, consultants, customers and third-party payors subject us to various federal and state fraud and abuse laws and other healthcare laws, including, without limitation, the federal Anti-Kickback Statute, the federal civil and criminal false claims laws, HIPAA and regulations promulgated under such laws. These laws will impact, among other things, our clinical research, proposed sales, marketing and educational programs, and other interactions with healthcare professionals. For more information regarding the risks related to these laws and regulations please see “Business – Regulatory Matters – U.S. Federal and State Fraud and Abuse Laws.” The scope and enforcement of each of these laws is uncertain and subject to rapid change in the current environment of healthcare reform. Federal and state enforcement bodies have recently increased their scrutiny of interactions between healthcare companies and healthcare providers, which has led to a number of investigations, prosecutions, convictions and settlements in the healthcare industry. Because of the breadth of these laws and the narrowness of their statutory or regulatory exceptions and safe harbors, some of our business activities may be subject to challenge under one or more of them. Ensuring that our internal operations and future business arrangements with third parties comply with applicable healthcare laws and regulations will involve substantial costs. Achieving and sustaining compliance requires us to implement controls across our entire organization which may prove costly and challenging to monitor and enforce. The risk of our being found in violation of healthcare laws and regulations is increased by the fact that their provisions are sometimes complex and open to a variety of interpretations. It is possible that governmental authorities will conclude that our business practices do not comply with current or future statutes, regulations, agency guidance or case law involving applicable fraud and abuse or other healthcare laws and regulations. If our operations are found to be in violation of any of the laws described above or any other governmental laws and regulations that may apply to us, we may be subject to significant penalties, including administrative, civil and criminal penalties, damages, fines, disgorgement, the exclusion from participation in federal and state healthcare programs, individual imprisonment, reputational harm, and the curtailment or restructuring of our operations, as well as additional reporting obligations and oversight if we become subject to a corporate integrity agreement or other agreement to resolve allegations of non-compliance with these laws. Likewise, if any of the physicians or other providers or entities with whom we expect to do business are found to not be in compliance with applicable laws, they may be subject to criminal, civil or administrative sanctions, including exclusions from government funded healthcare programs and imprisonment as well. Further, defending against any such actions can be costly and time consuming, and may require significant financial and personnel resources. Therefore, even if we are successful in defending against any such actions that may be brought against us, our business may be impaired. If any of the above occur, our ability to operate our business and our results of operations could be adversely affected. The U.S. Food and Drug Administration may in the future determine that our technology solutions are subject to the Federal Food, Drug, and Cosmetic Act and we may face additional costs and risks as a result. The FDA may promulgate a policy or regulation that affects our products and services. FDA regulations govern among other things, product development, testing, manufacture, packaging, labeling, storage, clearance or approval, advertising and promotion, sales and distribution and import and export for regulated drugs, biologics and devices. Non-compliance with applicable FDA requirements can result in, among other things, public warning letters, fines, injunctions, civil penalties, recall or seizure of products, total or partial suspension of production, failure of the FDA to grant marketing approvals, withdrawal of marketing approvals, a recommendation by the FDA to disallow us from entering into government contracts and criminal prosecutions. The FDA also has the authority to request repair, replace or refund of the cost of any device. Individuals may claim our calling or text messaging services are subject to, and are not compliant with the Telephone Consumer Protection Act or similar state laws. Our clients may use our products to place various short message service, or SMS, text messages and calls to patients. The Telephone Consumer Protection Act (“TCPA”) is a federal statute that protects consumers from unwanted telephone calls, faxes and text messages. There are a number of federal and state statutes and regulations that govern such telecommunications, the use of automatic telephone dialing systems (“ATDS”) or other automated systems to make such telecommunications, and the use of artificial voice or pre-recorded messages in certain telecommunications. These laws include the Telephone Consumer Protection Act (TCPA), Telemarketing Sales Rule (TSR), and various other state laws. The U.S. Federal Communications Commission (FCC), and the Federal Trade Commission have responsibility for regulating various aspects of some of the TCPA, TSR and other federal laws. Among other requirements, the TCPA requires callers to obtain prior express written consent for certain telemarketing calls and to adhere to “do-not-call” registry requirements which, in part, mandate that callers maintain and regularly update lists of consumers who have chosen not to be called and restrict calls to consumers who are on the national do-not-call list. Florida, Oklahoma and other states also have mini-TCPA and other similar consumer protection laws regulating calls and texts directed to their residents. As currently construed, the TCPA does not distinguish between voice and data, and, as such, text and SMS / MMS messages are also “calls” for the purpose of TCPA (and, in some cases, state mini-TCPA) obligations and restrictions. For violations of the TCPA, the law provides for a private right of action under which a plaintiff may recover monetary damages of \$ 500 for each call or text made in violation of the prohibitions on certain calls made using an artificial or pre-recorded voice or an ATDS and certain calls made to numbers properly registered on the federal “do-not-call” list. A court may treble the \$ 500 amount upon a finding of a willful or knowing violation. There is no statutory cap on maximum aggregate exposure (although some courts have applied in TCPA class actions constitutional limits on excessive penalties). An action may be brought by the FCC, a state attorney general, an individual, or a class of individuals. As with the

TCPA, Florida's mini- TCPA, for example, restricts certain calls and calls and texts made using an automated system to Florida residents without prior consent, allows a plaintiff to obtain \$ 500 for each call or text made in violation of its prohibitions, and permits a court to treble the \$ 500 amount for willful or knowing violations of the statute. The TCPA, TSR, mini- TCPA laws and other similar state laws are subject to interpretations that may change. We regularly evaluate how they may apply to our business. The FCC, FTC, a state attorney general or other regulator, or a court, however, may disagree with our interpretation of these laws and conclude that we are not in compliance and impose damages, civil penalties and other consequences upon us for noncompliance. Determination by a court or regulatory agency that our services did not comply also invalidate all or portions of some of our client contracts, could require us to change or terminate some portions of our business, could require us to refund portions of our services fees, and could have an adverse effect on our business. Further, we could be subject to putative class action lawsuits alleging violations of the TCPA, state mini- TCPA laws and other similar state laws. Our call and SMS texting services are potential sources of risk for class action lawsuits and liability for our Company. Numerous class- action suits under federal and state laws have been filed in recent years against companies who conduct call and SMS texting programs, with many resulting in multi- million- dollar settlements to the plaintiffs. Even an unsuccessful challenge by consumers or regulatory authorities of our activities could result in adverse publicity and could require a costly response from us. If in the future we are found to have violated such laws in a class action, the amount of damages and potential liability could be extensive and adversely impact our business. Accordingly, were such a class certified or if we are unable to successfully defend such a suit, then the damages could have a material adverse effect on our results of operations and financial condition. **Artificial**

intelligence presents risks and challenges that can impact our business including by posing security risks to our confidential information, proprietary information, and personal data. Issues in the development and use of artificial intelligence, combined with an uncertain regulatory environment, may result in reputational harm, liability, or other adverse consequences to our business operations. As with many technological innovations, artificial intelligence presents risks and challenges that could impact our business. We may adopt and integrate generative artificial intelligence tools into our systems for specific use cases reviewed by legal and information security. Our vendors may incorporate generative artificial intelligence tools into their offerings without disclosing this use to us, and the providers of these generative artificial intelligence tools may not meet existing or rapidly evolving regulatory or industry standards with respect to privacy and data protection and may inhibit our or our vendors' ability to maintain an adequate level of service and experience. If we, our vendors, or our third- party partners experience an actual or perceived breach or privacy or security incident because of the use of generative artificial intelligence, we may lose valuable intellectual property and confidential information and our reputation and the public perception of the effectiveness of our security measures could be harmed. Further, bad actors around the world use increasingly sophisticated methods, including the use of artificial intelligence, to engage in illegal activities involving the theft and misuse of personal information, confidential information, and intellectual property. Any of these outcomes could damage our reputation, result in the loss of valuable property and information, and adversely impact our business.

Our employees in Canada are subject to the laws and regulations of the government of Canada and its subdivisions. Certain of our employees are based in Canada and are subject to additional laws and regulations by the government of Canada, as well as its provinces. These include Canadian federal and local corporation requirements, restrictions on exchange of funds, employment- related laws and qualification for tax status. If we fail to comply with Canadian laws and regulations, or if the government of Canada or its provinces determines that our corporate actions do not comply with applicable Canadian law, we could face sanctions or fines, which could have a material adverse effect on our business. Due to the particular nature of certain services we provide or the manner in which we provide them, we may be subject to additional government regulation and foreign government regulation. While our **Platform is solutions are** primarily subject to government regulations pertaining to healthcare, certain aspects of our **Platform solutions** may require us to comply with regulatory schema from other areas. Examples of such regulatory schema include: • Foreign Corrupt Practices Act ("FCPA") and foreign anti- bribery laws. The FCPA makes it illegal for U. S. persons, including U. S. companies, and their subsidiaries, directors, officers, employees, and agents, to promise, authorize or make any corrupt payment, or otherwise provide anything of value, directly or indirectly, to any foreign official, any foreign political party or party official, or candidate for foreign political office to obtain or retain business. Violations of the FCPA can also result in violations of other U. S. laws, including anti- money laundering, mail and wire fraud, and conspiracy laws. There are severe penalties for violating the FCPA. **The** In addition, the Company may also be subject to other non- U. S. anti- corruption or anti- bribery laws, such as the U. K. Bribery Act 2010. If our employees **In many foreign countries**, particularly in those contractors, vendors, or partners fail to comply with **developing economies, it may be common to engage in business practices that are prohibited by laws and regulations applicable to us, such as** the FCPA and other /or foreign anti- bribery laws. Any violations of the FCPA or **local anti- corruption laws by us**, we may be subject to **our subsidiaries or our local agents in India or elsewhere could have a material adverse effect on our business, financial condition, results of operations, and prospects, as well as our reputation, and result in substantial financial** penalties or **other** sanctions, and our ability to develop new prospects and retain existing customers could be adversely affected. • Economic sanctions and export controls. Economic and trade sanctions programs that are administered by the U. S. Treasury Department's Office of Foreign Assets Control (OFAC) prohibit or restrict transactions to or from, and dealings with specified countries and territories, their governments, and in certain circumstances, with individuals and entities that are located in or nationals of those countries, and other sanctioned persons, including specially designated nationals, narcotics traffickers and terrorists or terrorist organizations. As federal, state and foreign legislative regulatory scrutiny and enforcement actions in these areas increase, we expect our costs to comply with these requirements will increase as well. Failure to comply with any of these requirements could result in the limitation, suspension or termination of our services, imposition of significant civil and criminal penalties, including fines, and / or the seizure and / or forfeiture of our assets. • Further, our **Platform solutions** incorporate **incorporate** encryption technology. The U. S. Export

and regulations of the government of Canada and its subdivisions. Certain of our employees are based in Canada and are subject to additional laws and regulations by the government of Canada, as well as its provinces. These include Canadian federal and local corporation requirements, restrictions on exchange of funds, employment- related laws and qualification for tax status. If we fail to comply with Canadian laws and regulations, or if the government of Canada or its provinces determines that our corporate actions do not comply with applicable Canadian law, we could face sanctions or fines, which could have a material adverse effect on our business. Due to the particular nature of certain services we provide or the manner in which we provide them, we may be subject to additional government regulation and foreign government regulation. While our **Platform is solutions are** primarily subject to government regulations pertaining to healthcare, certain aspects of our **Platform solutions** may require us to comply with regulatory schema from other areas. Examples of such regulatory schema include: • Foreign Corrupt Practices Act ("FCPA") and foreign anti- bribery laws. The FCPA makes it illegal for U. S. persons, including U. S. companies, and their subsidiaries, directors, officers, employees, and agents, to promise, authorize or make any corrupt payment, or otherwise provide anything of value, directly or indirectly, to any foreign official, any foreign political party or party official, or candidate for foreign political office to obtain or retain business. Violations of the FCPA can also result in violations of other U. S. laws, including anti- money laundering, mail and wire fraud, and conspiracy laws. There are severe penalties for violating the FCPA. **The** In addition, the Company may also be subject to other non- U. S. anti- corruption or anti- bribery laws, such as the U. K. Bribery Act 2010. If our employees **In many foreign countries**, particularly in those contractors, vendors, or partners fail to comply with **developing economies, it may be common to engage in business practices that are prohibited by laws and regulations applicable to us, such as** the FCPA and other /or foreign anti- bribery laws. Any violations of the FCPA or **local anti- corruption laws by us**, we may be subject to **our subsidiaries or our local agents in India or elsewhere could have a material adverse effect on our business, financial condition, results of operations, and prospects, as well as our reputation, and result in substantial financial** penalties or **other** sanctions, and our ability to develop new prospects and retain existing customers could be adversely affected. • Economic sanctions and export controls. Economic and trade sanctions programs that are administered by the U. S. Treasury Department's Office of Foreign Assets Control (OFAC) prohibit or restrict transactions to or from, and dealings with specified countries and territories, their governments, and in certain circumstances, with individuals and entities that are located in or nationals of those countries, and other sanctioned persons, including specially designated nationals, narcotics traffickers and terrorists or terrorist organizations. As federal, state and foreign legislative regulatory scrutiny and enforcement actions in these areas increase, we expect our costs to comply with these requirements will increase as well. Failure to comply with any of these requirements could result in the limitation, suspension or termination of our services, imposition of significant civil and criminal penalties, including fines, and / or the seizure and / or forfeiture of our assets. • Further, our **Platform solutions** incorporate **incorporate** encryption technology. The U. S. Export

Administration Regulations require authorization for the export of certain encryption items, including by a license, a license exception or other appropriate government authorizations. Such solutions may also be subject to certain regulatory reporting requirements. While we believe our products meet certain exceptions that reduce the scope of export control restrictions applicable to such products, these exceptions may be determined not to apply to our products and our products and underlying technology may become subject to export control restrictions. **• In addition, our establishment of a subsidiary in India and our plans to bring outside services in-house through that entity could increase our risk of violations of such laws and regulations in the future. Despite our policies, procedures and compliance programs, our internal controls and compliance systems may not be able to protect us from prohibited acts willfully committed by our employees, agents or business partners that would violate such applicable laws and regulations.** Risks relating to our dependence on third parties

We rely on our third-party contractors, vendors and partners, including some outside of the United States, to execute our business strategy. Replacing them could be difficult and disruptive to our business. If we are unsuccessful in forming or maintaining such relationships on terms favorable to us, our business may not succeed. We have entered into contracts with third-party contractors and vendors to provide critical services relating to our business, including initial software development and cloud hosting. We also rely on third-party providers to enable automated eligibility and benefits verification through our **Platform solutions**, and we outsource certain of our software development and design, quality assurance and operations activities to third-party contractors that have employees and consultants in international locations that may be subject to political and economic instability, including India, ~~Russia~~ and Ukraine. ~~For example, we have entered into a Master Services Agreement with Rayden, pursuant to which Rayden's India-based personnel exclusively support our business through various functions including, but not limited to finance and accounting, sales and marketing, customer operations, product management and support, and research and development. We are also a party to a Consulting and Development Agreement with DataArt, pursuant to which we primarily outsource certain software development services to DataArt.~~ Our dependence on ~~Rayden, DataArt and other~~ third-party contractors to support key functions of our business creates numerous risks, in particular, the risk that we may not maintain service quality, control or effective management with respect to these operations. In the event that these service providers fail to maintain adequate levels of support, do not provide high quality service, increase the fees they charge us, discontinue their lines of business, terminate our contractual arrangements or cease or reduce operations, we may suffer additional costs and be required to pursue new third-party relationships, which could materially disrupt our operations and our ability to provide our products and services, and could divert management's time and resources. Our reputation and our customers' willingness to purchase our products and partners' willingness to use our products depend, in part, on our third-party contractors' compliance with ethical employment practices, such as with respect to child labor, wages and benefits, forced labor, discrimination, safe and healthy working conditions, and with all legal and regulatory requirements relating to the conduct of their businesses. If our third-party contractors fail to comply with applicable laws, regulations, safety codes, employment practices, human rights standards, quality standards, environmental standards, production practices, or other obligations, norms, or ethical standards, our reputation and brand image could be harmed and we could be exposed to litigation and additional costs that would harm our business, reputation, and results of operations. **These third-party contractors, some of which handle sensitive data on our behalf, could be non-compliant with regulatory requirements or our contractual provisions regarding the handling of sensitive data, despite our best efforts to monitor their compliance and mitigate risks in our contractual cost-shifting provisions. Even if these third parties are compliant, they still could be the victims of sophisticated cyberattacks or other unforeseeable events.** The ability of our third-party contractors to effectively satisfy our business requirements could be impacted by financial difficulty of our third-party contractors or damage to their operations caused by fire, terrorist attack, natural disaster, or other events. It would be difficult to replace some of our third-party contractors and third-party vendors in a timely manner if they were unwilling or unable to provide us with these services in the future, and our business and operations could be adversely affected. If these services fail or are of poor quality, our business, reputation and operating results could be harmed. For example, the continued Russian invasion of Ukraine has, and may continue to, impact macroeconomic conditions, give rise to regional instability, increase the threat of cyberwarfare and result in heightened economic sanctions from the U. S. and the international community in a manner that adversely affects us and our third-party contractors that have employees and consultants located in ~~Russia and~~ Ukraine. Further, although the length and impact of the continuing conflict are highly unpredictable, individuals located in these areas have been and could continue to be forced to evacuate or voluntarily choose to relocate, making them unavailable to provide services, such as software engineering, to support our business. It could also disrupt or delay our communications with such resources or the flow of funds to support their operations, or otherwise render some of our resources unavailable. While we have risk mitigation efforts in place, the realization of any **of** these risks could adversely affect our product development, operations, business and / or financial results and may require us to shift some of our development activities to other jurisdictions and / or third-party contractors, which may result in significant disruption, including delays in releases of new versions or updates of our software and incurrence of additional costs. We anticipate that we will continue to depend on these and other third-party relationships in order to grow our business for the foreseeable future. If we are unsuccessful in maintaining existing and, if needed, establishing new relationships with third parties, our ability to efficiently operate existing services or develop new services could be impaired, and, as a result, our competitive position or our results of operations could suffer. We also depend on our third-party processing partners to perform payment processing services, which generate almost all of our payments revenue. Our processing partners may go out of business or otherwise be unable or unwilling to continue providing such services, which could significantly and materially reduce our payments revenue and disrupt our business. A number of our processing contracts require us to assume liability for any losses our processing partners may suffer as a result of losses caused by our healthcare services clients and their patients, including losses caused by chargebacks and fraud. Thus, in the event of a significant loss by our processing partners, we may be required to pay-out a large amount of cash in one or two business days following such event and, if we do not have sufficient

cash on hand, may be deemed in breach of such contracts. A contractual dispute with our processing partners could adversely impact our revenue. Certain contracts may expire or be terminated, and we may not be able to enter into a new payment processor relationship that replicates the associated revenue for a considerable period of time. In addition, we have entered into contracts with providers of EHR and PM solutions, and we intend to pursue such agreements in the future. These contracts are typically structured as commercial and technical agreements, pursuant to which we integrate certain of our ~~Platform~~ solutions into the EHR and PM systems that are utilized by many of our clients, for agreed payments or provision of services to such providers of EHR and PM solutions. Our ability to form and maintain these agreements in order to facilitate the integration of our ~~Platform~~ solutions into the EHR and PM systems used by our healthcare services clients and their patients is important to the success of our business. If providers of EHR or PM solutions amend, terminate or fail to perform their obligations under their agreements with us, we may need to seek other ways of integrating our ~~Platform~~ solutions with the EHR and PM systems of our healthcare services clients, which could be costly and time consuming, and could adversely affect our business results. We or the providers of EHR and PM solutions with which we contract may terminate or seek to amend our agreements in order to incorporate ~~new~~ the final ~~Final rules~~ Rules promulgated ~~in~~ on March 9, 2020 by the HHS, ONC, and CMS, which ~~are~~ is further described above and ~~are~~ is aimed at supporting seamless and secure access, exchange, and use of EHI by increasing innovation and competition by giving patients and their healthcare service providers secure access to health information and new tools, allowing for more choice in care and treatment. We may also seek to enter into new agreements in the future, and we may not be successful in entering into future agreements on terms favorable to us. Any delay in entering agreements with providers of EHR or PM solutions or other technology providers could either delay the development and adoption of our products and services and reduce their competitiveness. Any such delay could adversely affect our business. We rely on a limited number of third- party suppliers and contract manufacturers to support our products, and a loss or degradation in performance of these suppliers and contract manufacturers could have a negative effect on our business, financial condition and results of operations. We rely on third- party suppliers and contract manufacturers for the materials and components used to operate our ~~solutions~~ Phreesia ~~Platform~~ and product offerings, and to manufacture and assemble our hardware, including the PhreesiaPad and our on- site kiosks, which we refer to as Arrivals Kiosks. We rely on a sole supplier, for example, as the manufacturer of our PhreesiaPads and Arrivals Kiosks, which help drive our business and support our subscription, payment processing and life sciences offerings. In connection with these services, our supplier builds new hardware for us and refurbishes and maintains existing hardware. Any of our other suppliers or third- party contract manufacturers may be unwilling or unable to supply the necessary materials and components or manufacture and assemble our products reliably and at the levels we anticipate or that are required by the market. Our ability to supply our products commercially and to develop any future products depends, in part, on our ability to obtain these materials, components and products in accordance with regulatory requirements and in sufficient quantities for commercialization. If we are required to change contract manufacturers due to any change in or termination of our relationships with these third parties, or if our manufacturers are unable to obtain the materials they need to produce our products at consistent prices or at all, (including, without limitation, because of the effect of tariffs or other trade restrictions), we may lose sales, experience manufacturing or other delays, incur increased costs or otherwise experience impairment to our client relationships. We cannot guarantee that we will be able to establish alternative relationships on similar terms, without delay or at all. If our third- party suppliers fail to deliver the required quantities of materials on a timely basis and at commercially reasonable prices, and we are unable to find one or more replacement suppliers capable of production at a substantially equivalent cost in substantially equivalent volumes and quality on a timely basis, the supply of our products to clients and the development of any future products will be delayed, limited or prevented, which could have material adverse effect on our business, financial condition and results of operations. We rely on Internet infrastructure, bandwidth providers, data center providers, other third parties and our own systems for providing services to our clients, and any failure or interruption in the services provided by these third parties or our own systems could expose us to litigation and negatively impact our relationships with clients, adversely affecting our brand and our business. Our ability to deliver our products and services, particularly our cloud- based solutions, is dependent on the development and maintenance of the infrastructure of the Internet and other telecommunications services by third parties. This includes maintenance of a reliable network connection with the necessary speed, data capacity and security for providing reliable Internet access and services and reliable telephone and facsimile services. Our services are designed to operate without interruption in accordance with our service level commitments. However, we have experienced limited interruptions in these systems in the past, including server failures that temporarily slow down the performance of our services, and we may experience more significant interruptions in the future. We rely on internal systems as well as third- party suppliers, including bandwidth and telecommunications equipment providers, to provide our services. We do not maintain redundant systems or facilities for some of these services. Interruptions in these systems, whether due to system failures, computer viruses, physical or electronic ~~attacks~~ break-ins or other catastrophic events, could affect the security or availability of our services, ~~compromise the data we handle on behalf of our partners~~ and prevent or inhibit the ability of our partners to access our services. In the event of a catastrophic event with respect to one or more of these systems or facilities, we may experience an extended period of system unavailability, which could result in substantial costs to remedy those problems or negatively impact our relationship with our clients, our business, results of operations and financial condition. Any disruption in the network access, telecommunications or co- location services provided by third- party providers or any failure of or by third- party providers' systems or our own systems to handle current or higher volume of use could significantly harm our business. We exercise limited control over our third- party suppliers, which increases our vulnerability to problems with services they provide. We have experienced failures by third- party providers' systems which resulted in a limited interruption of our system, ~~although this failure did not result in any claims against us~~. Any errors, failures, interruptions or delays experienced in connection with these third- party technologies and information services or our own systems could negatively impact our relationships with clients and adversely affect our business and could expose us to third- party liabilities. The reliability and

performance of our Internet connection may be harmed by increased usage or by denial- of- service attacks. The Internet has experienced a variety of outages and other delays as a result of damages to portions of its infrastructure, and it could face outages and delays in the future. These outages and delays could reduce the level of Internet usage as well as the availability of the Internet to us for delivery of our Internet- based services. Risks relating to taxes and accounting standards Changes in tax regulations and accounting standards, or changes in related judgments or assumptions could materially impact our financial position and results of operation. We are subject to federal and state income, sales, use, value added and other taxes in the United States and other countries in which we conduct business, and such laws and rates vary by jurisdiction. We are now registered in all states that assess sales taxes on our services. Although we believe our tax practices and provisions are reasonable, the final determination of tax audits and any related litigation, changes in the taxation of our activities and proposed changes in tax laws could cause the ultimate settlement of our tax liabilities to be materially different from our historical tax practices, provisions and accruals. If we receive an adverse ruling as a result of an audit, or we unilaterally determine that we have misinterpreted provisions of the tax regulations to which we are subject, there could be a material effect on our tax provision, net income or cash flows in the period or periods for which that determination is made, which could materially impact our financial results. Further, any changes in the taxation of our activities, including certain proposed changes in U. S. tax laws, may increase our effective tax rate and adversely affect our financial position and results of operations. In addition, liabilities associated with taxes are often subject to an extended or indefinite statute of limitations period. Therefore, we may be subject to additional tax liability (including penalties and interest) for a particular year for extended periods of time. Furthermore, changes in accounting rules and interpretations or in our accounting assumptions and / or judgments could significantly impact our consolidated financial statements. In some cases, we could be required to delay the filing of our consolidated financial statements, or to apply a new or revised standard retroactively, resulting in restating prior period consolidated financial statements. Any of these circumstances could have a material adverse effect on our business, prospects, liquidity, financial condition and results of operations. Our ability to use our net operating losses to offset future taxable income may be subject to certain limitations. As of January 31, 2023, we had U. S. federal and state net operating loss carryforwards ~~of~~ ("NOLs") of \$ 493,599,300 million due to prior period losses, which, subject to the following discussion, are generally available to be carried forward to offset a portion of our future taxable income, if any, until such NOLs are used or expire. In general, under Section 382 ("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 pre- ownership change NOLs to offset future taxable income. Similar rules may apply under state tax laws. We have completed a Section 382 study and as a result of the analysis, it is more likely than not that we have experienced an "ownership change." In addition, it is more likely than not that our existing NOLs are subject to limitations arising from previous ownership changes. Future changes in our stock ownership, some of which are outside of our control, could result in an ownership change under Section 382 of the Code. In addition, under the Tax Cuts and Jobs Act of 2017, as amended by The Coronavirus Aid, Relief, and Economic Security Act of 2020, the amount of post 2017 NOLs that we are permitted to utilize in any taxable year is limited to 80 % of our taxable income in such year, where taxable income is determined without regard to the NOL deduction itself. For these reasons, we may not be able to realize a tax benefit from the use of our NOLs. We have a valuation allowance related to our NOLs to recognize only the portion of the deferred tax asset that is more likely than not to be realized. Risks relating to our financing needs Our cash and cash equivalents could be adversely affected if the financial institutions in which we hold our cash and cash equivalents fail. We regularly maintain cash balances at third- party financial institutions in excess of the Federal Deposit Insurance Corporation ("FDIC") insurance limit, **and there can be no assurance that we will be able to access uninsured funds in a timely manner or at all in the event of a failure of these financial institutions.** If any such depository institution fails to return our deposits, or if a depository institution is subject to other adverse conditions in the financial or credit markets, this could further impact access to our invested cash or cash equivalents and could adversely impact our operating liquidity and financial performance. In order to support the growth of our business, we may need to incur additional indebtedness under our current credit facilities or seek capital through new equity or debt financings, which sources of additional capital may not be available to us on acceptable terms or at all. Our operations have consumed substantial amounts of cash since inception and we intend to continue to make significant investments to support our business growth, respond to business challenges or opportunities, develop new applications and services, enhance our existing solution and services, enhance our operating infrastructure and potentially acquire complementary businesses and technologies. For the year ended January 31, 2023-2024 our net cash used in operating activities was \$ 90,321,400 million. As of January 31, 2023-2024, we had \$ 176,877,750 million of cash and cash equivalents, which are held for working capital purposes. ~~We are~~ **Prior to its termination on December 4, 2023, we were** party to a credit facility with Silicon Valley Bank ("SVB") pursuant to which we ~~have had~~ the ability to borrow up to \$ 100.0 million under a revolving line of credit. ~~The~~ **On December 4, 2023, we entered into a credit agreement (the "Credit Agreement") with Capital One, National Association ("Capital One"), providing for a senior secured asset-based revolving** credit facility ~~contains a covenant limiting our ability to retain certain levels of cash in accounts outside SVB. As of January 31, 2023, we were in compliance with all covenants in the credit facility. However, in connection with the closure of SVB, we transferred substantially all of our cash and~~ **an initial borrowing capacity of** cash equivalents from SVB to other financial institutions. ~~On Friday March 10, 2023, we obtained consent from SVB to retain up to \$ 165,50.0 million (of cash outside SVB until May 15, 2023 provided we do not borrow against the " Capital One credit Credit facility Facility ")~~ **As a result, we** ~~Our obligations under the Capital One Credit Facility are guaranteed by~~ **unable to borrow against our subsidiaries located in** ~~credit facility until we return sufficient cash and cash equivalents to SVB to comply with the covenant discussed above and maintain compliance with the other~~ **the United States, and** ~~covenants in the credit facility. Borrowings under the facility are secured by a first priority lien on~~ **substantially all of our tangible properties, rights and intangible assets, excluding intellectual property.** As of January 31, 2023-2024, we had no outstanding borrowings under **the Capital One** ~~our revolving line of credit~~

Credit Facility. Our future capital requirements may be significantly different from our current estimates and will depend on many factors, including the need to: • finance unanticipated working capital requirements; • develop or enhance our technological infrastructure and our existing products and services; • fund strategic relationships, including joint ventures and co- investments; • fund additional implementation engagements; • respond to competitive pressures; and • acquire complementary businesses, technologies, products or services. Accordingly, we may need to engage in equity or debt financings or collaborative arrangements to secure additional funds. Additional financing may not be available on terms favorable to us, or at all. If we raise additional funds through further 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 secured by us in the future could involve additional 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. In addition, during times of economic instability, it has been difficult for many companies to obtain financing in the public markets or to obtain debt financing, and we may not be able to obtain additional financing on commercially reasonable terms, if at all. If we are unable to obtain adequate financing or financing on terms satisfactory to us, it could have a material adverse effect on our business, financial condition and results of operations. Restrictive covenants in the agreements governing our **Capital One credit-Credit facility-Facility** may restrict our ability to pursue our business strategies. The ~~credit-Credit agreement-Agreement~~ governing our **Capital One credit-Credit facility-Facility** with SVB contains **various**, and any future credit agreements we may enter into may contain, restrictive covenants that limit our ability to **take certain actions, including, but not limited to, our ability to grant or incur liens, dispose of assets**, incur additional indebtedness and liens, merge with other companies or consummate certain changes of control, acquire other companies, engage in new lines of business, make certain investments, **pay-restricted payments (including dividends)**, create subsidiaries and restricted debt payments, enter into certain transactions with affiliates, and transfer or dispose of assets as well as **enter into certain mergers and acquisitions. In addition, the Capital One Credit Facility contains** financial covenants requiring us **applicable from time to time** maintain a specified level of recurring revenue growth, **which include** a specified maximum funded debt to recurring revenue ratio and a specified amount of minimum **Minimum Consolidated EBITDA, Consolidated Fixed Charge Coverage Ratio and Minimum liquidity Liquidity**, as such terms are defined in the Credit Agreement. Our ability to comply with these covenants **and meet these financial ratios and tests** may be affected by events beyond our control, and we may not be able to meet those covenants. A breach of any of any such covenants could result in a default under the applicable loan agreement, which could cause all of the outstanding indebtedness under such credit facility to become immediately due and payable and terminate all commitments to extend further credit. These covenants could also limit our ability to seek capital through the incurrence of new indebtedness or, if we are unable to meet our obligations, require us to repay any outstanding amounts with sources of capital we may otherwise use to fund our business, operations and strategy. Adverse developments affecting the financial services industry, such as actual events or concerns involving liquidity, defaults or non- performance by financial institutions or transactional counterparties, could adversely affect our current and projected business operations and our financial condition and results of operations. Adverse developments that affect financial institutions, transactional counterparties or other third parties, or concerns or rumors about any events of these kinds or other similar risks, have in the past and may in the future lead to market- wide liquidity problems. For example, on March 10, 2023, SVB was closed by the California Department of Financial Protection and Innovation, which appointed the FDIC as receiver. Similarly, on March 12, 2023, Signature Bank and Silvergate Capital Corp. were each swept into receivership. The U. S. Department of the Treasury, the Federal Reserve and the FDIC released a statement that indicated that all depositors of SVB would have access to all of their money after only one business day of closure, including funds held in uninsured deposit accounts. We had a minimal amount of exposure to the SVB closure and did not experience any adverse impact to our liquidity or to our current and projected business operations, financial condition or results of operations. However, uncertainty remains over liquidity concerns in the broader financial services industry, and there may be additional impacts to our business and our industry that we cannot predict. Similar impacts have occurred in the past, such as during the 2008-2010 financial crisis. Inflation and rapid increases in interest rates have led to a decline in the trading value of previously issued government securities with interest rates below current market interest rates. Although the U. S. Department of Treasury, FDIC and Federal Reserve Board have announced a program to provide up to \$ 25 billion of loans to financial institutions secured by certain of such government securities held by financial institutions to mitigate the risk of potential losses on the sale of such instruments, widespread demands for customer withdrawals or other liquidity needs of financial institutions for immediately liquidity may exceed the capacity of such program. There is no guarantee that the U. S. Department of Treasury, FDIC and Federal Reserve Board will provide access to uninsured funds in the future in the event of the closure of other banks or financial institutions, or that they would do so in a timely fashion. Although we assess our banking relationships as we believe necessary or appropriate, our access to cash in amounts adequate to finance or capitalize our current and projected future business operations could be significantly impaired by factors that affect us, the financial institutions with which we have banking relationships, or the financial services industry or economy in general. These factors could include, among others, events such as liquidity constraints or failures, the ability to perform obligations under various types of financial, credit or liquidity agreements or arrangements, disruptions or instability in the financial services industry or financial markets, or concerns or negative expectations about the prospects for companies in the financial services industry. These factors could involve financial institutions or financial services industry companies with which we have financial or business relationships, but could also include factors involving financial markets or the financial services industry generally. The results of events or concerns that involve one or more of these factors could include a variety of material and adverse impacts on our current and projected business operations and our financial condition and results of operations. These could include, but may not be limited to, the following: • delayed access to deposits or other financial assets or the uninsured loss of deposits or other financial assets;

• loss of access to revolving existing credit facilities or other working capital sources and / or the inability to refund, roll over or extend the maturity of, or enter into new credit facilities or other working capital resources; or • potential or actual breach of financial covenants in our credit agreements or credit arrangements. ~~In addition, widespread~~ **Widespread** investor concerns regarding the U. S. or international financial systems could **also** result in less favorable commercial financing terms, including higher interest rates or costs and tighter financial and operating covenants, or systemic limitations on access to credit and liquidity sources, thereby making it more difficult for us to acquire financing on acceptable terms or at all. Any decline in available funding or access to our cash and liquidity resources could, among other risks, adversely impact our ability to meet our operating expenses, financial obligations or fulfill our other obligations, result in breaches of our financial and / or contractual obligations or result in violations of federal or state wage and hour laws. Any of these impacts, or any other impacts resulting from the factors described above or other related or similar factors not described above, could have material adverse impacts on our liquidity and our current and / or projected business operations and financial condition and results of operations. In addition, a partner or supplier could be adversely affected by any of the liquidity or other risks that are described above as factors that could result in material adverse impacts on the Company, including but not limited to delayed access or loss of access to uninsured deposits or loss of the ability to draw on existing credit facilities involving a troubled or failed financial institution. Any partner or supplier bankruptcy or insolvency, or the failure of any partner to make payments when due, or any breach or default by a partner or supplier, or the loss of any significant supplier relationships, may have a material adverse impact on our business. Risks relating to ownership of our common stock Our share price has been and may in the future be volatile, and you could lose all or part of your investment. The trading price of our common stock has been and may be volatile and subject to wide price fluctuations in response to various factors, including, but not limited to: • market conditions in the broader stock market in general, or in our industry in particular, which create highly variable and unpredictable pricing of equity securities; • actual or anticipated fluctuations in our quarterly financial reports and results of operations; • changes in the financial projections we provide to the public or our failure to meet these projections; • our ability to satisfy our ongoing capital needs and unanticipated cash requirements; • indebtedness incurred in the future; • actual or anticipated developments in our business, our competitors' businesses, or the competitive landscape generally, including introduction of new products and services by us or our competitors; • issuance of new or changed securities analysts' reports or recommendations; • additions or departures of key personnel; • new laws or regulations or new interpretations of existing laws or regulations applicable to our business; • regulatory developments; • litigation and governmental investigations; • the impact of ~~COVID-19~~ **public health concerns** on the economy, our company, our customers, suppliers or employees; • macroeconomic conditions, such as rising interest and inflation rates and economic slowdowns and recessions, and political conditions or events, including those resulting from geopolitical uncertainty and instability or war, such as the ongoing military conflict between Russia and Ukraine **and the conflict in the Middle East**; and • our sale of common stock or other securities in the future. In addition, on March 10, 2023, the FDIC took control and was appointed receiver of SVB. At the time SVB entered into receivership, a large number of companies, including many technology companies, held cash deposits with SVB. Although such companies had access to their deposits as of March 13, 2023, companies may continue to face financing uncertainty as a result of SVB's entry into receivership, which may cause significant volatility with respect to technology company stocks. This, in turn, could negatively impact the trading price of our common stock. These and other factors may cause the market price and demand for our common stock to fluctuate substantially, which may limit or prevent investors from readily selling their shares of common stock and may otherwise negatively affect the liquidity of our common stock. In addition, in the past, when the market price of a stock has been volatile, holders of that stock have instituted securities class action litigation against the company that issued the stock. If any of our stockholders brought a lawsuit against us, we could incur substantial costs defending the lawsuit. Such a lawsuit could also divert the time and attention of our management from our business. The trading market for our common stock is also influenced by the research and reports that industry or securities analysts publish about us or our business. If one or more securities or industry analysts cease coverage of our company or fail to publish reports on us regularly, we could lose visibility in the financial markets, which in turn could cause our stock price or trading volume to decline. If one or more of the analysts who cover us downgrades our common stock or provides more favorable recommendations about our competitors, or if our results of operations do not meet their expectations, our stock price could decline. We do not currently intend to pay dividends on our common stock and, consequently, your ability to achieve a return on your investment will depend on appreciation in the price of our common stock. We have never declared or paid any cash dividends on our common stock and do not currently intend to do so for the foreseeable future. We currently intend to invest our future earnings, if any, to fund our growth. Therefore, you are not likely to receive any dividends on your common stock for the foreseeable future and the success of an investment in shares of our common stock will depend upon any future appreciation in its value. There is no guarantee that shares of our common stock will appreciate in value or even maintain the price at which our stockholders have purchased their shares. Risks relating to our bylaws and certificate of incorporation Anti-takeover provisions under our incorporation documents and Delaware law could delay or prevent a change of control which could limit the market price of our common stock and may prevent or frustrate attempts by our stockholders to replace or remove our current management. Our **seventh** amended and restated certificate of incorporation (**as amended, our** "certificate of incorporation") and our ~~third~~ **fourth** amended and restated by-laws ("bylaws") contain provisions that could delay or prevent a change of control of our company or changes in our board of directors that our stockholders might consider favorable. Some of these provisions include: • a board of directors divided into three classes serving staggered three- year terms, such that not all members of the board will be elected at one time; • a prohibition on stockholder action through written consent, which requires that all stockholder actions be taken at a meeting of our stockholders; • a requirement that special meetings of stockholders be called only by the board of directors acting pursuant to a resolution approved by the affirmative vote of a majority of the directors then in office; • advance notice requirements for stockholder proposals and nominations for election to our board of directors; • a requirement that no member of our board of directors may

be removed from office by our stockholders except for cause and, in addition to any other vote required by law, upon the approval of not less than 75 % of all outstanding shares of our voting stock then entitled to vote in the election of directors; • a requirement of approval of not less than 75 % of all outstanding shares of our voting stock to amend any bylaws by stockholder action or to amend specific provisions of our certificate of incorporation; and • the authority of the board of directors to issue preferred stock on terms determined by the board of directors without stockholder approval and which preferred stock may include rights superior to the rights of the holders of common stock. In addition, because we are incorporated in Delaware, we are governed by the provisions of Section 203 of the Delaware General Corporate Law (" DGCL"), which may prohibit certain business combinations with stockholders owning 15 % or more of our outstanding voting stock. These anti- takeover provisions and other provisions in our certificate of incorporation and our bylaws could make it more difficult for stockholders or potential acquirers to obtain control of our board of directors or initiate actions that are opposed by the then- current board of directors and could also delay or impede a merger, tender offer or proxy contest involving our company. These provisions could also discourage proxy contests and make it more difficult for stockholders to elect directors or cause us to take other corporate actions. Any delay or prevention of a change of control transaction or changes in our board of directors could cause the market price of our common stock to decline. Our bylaws designate certain specified courts as the sole and exclusive forums for certain disputes between us and our stockholders, which could limit our stockholders' ability to obtain a favorable judicial forum for disputes with us or our directors, officers or employees. Our bylaws provide that, unless we consent in writing to the selection of an alternative forum, the Court of Chancery of the State of Delaware (the" Chancery Court") will be the sole and exclusive forum for state law claims for (i) any derivative action or proceeding brought on our behalf, (ii) any action asserting a claim of breach of a fiduciary duty owed by any of our directors, officers or other employees to us or our stockholders, (iii) any action asserting a claim pursuant to any provision of the DGCL, our certificate of incorporation or our bylaws, (iv) any action to interpret, apply, enforce or determine the validity of our certificate of incorporation or bylaws, or (v) any action asserting a claim governed by the internal affairs doctrine (the" Delaware Forum Provision"). The Delaware Forum Provision will not apply to any causes of action arising under the Securities Act of 1933, as amended (the" Securities Act"), or Securities Exchange Act of 1934, as amended, (the" Exchange Act"). Our bylaws further provide that, unless we consent in writing to the selection of an alternative forum, the federal district courts of the United States will be the sole and exclusive forum for resolving any complaint asserting a cause of action arising under the Securities Act (the" Federal Forum Provision"). Our bylaws provide that any person or entity purchasing or otherwise acquiring any interest in shares of our capital stock is deemed to have notice of and consented to the foregoing Delaware Forum Provision and the Federal Forum Provision; provided, however, that stockholders cannot and will not be deemed to have waived our compliance with the federal securities laws and the rules and regulations thereunder. The Delaware Forum Provision and the Federal Forum Provision in our bylaws may impose additional litigation costs on stockholders in pursuing any such claims. Additionally, these forum selection clauses may limit our stockholder' s ability to bring a claim in a judicial forum that it finds favorable for disputes with us or our directors, officers or other employees, which may discourage the filing of lawsuits against us and our directors, officers and employees, even though an action, if successful, might benefit our stockholders. In addition, while the Delaware Supreme Court and other states courts have upheld the validity of federal forum selection provisions purporting to require claims under the Securities Act be brought in federal court, there is uncertainty as to whether other courts will enforce our Federal Forum Provision. If the Federal Forum Provision is found to be unenforceable in an action, we may incur additional costs associated with resolving such an action. The Federal Forum Provision may also impose additional litigation costs on stockholders who assert that the provision is not enforceable or invalid. The Chancery Court or the federal district courts of the United States may also reach different judgments or results than would other courts, including courts where a stockholder considering an action may be located or would otherwise choose to bring the action, and such judgments may be more or less favorable to us than our stockholders.