Risk Factors Comparison 2024-03-29 to 2023-03-30 Form: 10-K

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

An investment in our securities involves a high degree of risk. You should carefully consider the risks and uncertainties described below and the other information contained in this Annual Report on Form 10- K before making an investment in our common stock. Our business, financial condition, results of operations or prospects could be materially and adversely affected if any of these risks occurs, and as a result, the market price of our common stock could decline, and you could lose all or part of your investment. Risks Related to our Business Operations We have a limited operating and financial history. We are ~~in the development stage~~ **an emerging growth company** and face all of the risks and uncertainties associated with ~~a new~~ **an early-stage** and unproven business ~~. Our future is based on an unproven business plan with no historical facts to support projections and assumptions~~ . We incorporated in October 2020 in anticipation of the Business Combination and had no operating history or revenues prior to their closing. We are faced with risks inherent in operating a new business, including difficulties often encountered in developing, producing and commercializing new technologies; developing the markets for our products and technologies; and attracting and retaining qualified management, sales and / or marketing and technical staff, in addition to the risks described below. We may need additional capital to fund our operations. We may require additional capital to fund our current operations and anticipated expansion of our business and to pursue targeted revenue opportunities. There is no assurance that additional capital to fund our operations can be raised. Additional capital may not be available, the terms of any such capital raising may be uncertain, and the terms of any prospective equity capital may not be acceptable. In addition, any future sale of equity securities would dilute the ownership and control of the then- current stockholders and could be at prices substantially below prices at which our shares currently trade or may trade. The inability to raise capital could require us to significantly curtail or terminate operations. We could lose our access to data from external sources, which could prevent us from providing our solutions. We depend upon data from external sources to create our information products. In general, we do not own the data that powers our information offerings. Our data sources could withdraw or increase the price for their data for a variety of reasons, and we could also become subject to legislative, judicial or contractual restrictions on the use of such data, in particular if such data are not collected by the third parties in a way that allows us to legally use and / or process the data. Additionally, the length of our licenses with our data suppliers and our ability to extend these licenses varies across suppliers, some of whom may offer similar products or services to certain categories of our customers and prospective customers. Our competitors could also enter into exclusive contracts with our data sources, which although atypical may preclude us from receiving certain data from these suppliers or restrict us in our use of such data, which would give our competitors an advantage. If a substantial number of data sources, or certain key sources, were to withdraw, limit or be unable to provide their data, or if we were to lose access to data due to government regulation or if the collection of data became uneconomical, our ability to provide our information solutions to our customers could be impacted, which could materially adversely affect our business, reputation, financial condition, operating results and cash flows. We may make ~~additional~~ acquisitions as a component of our growth strategy. We may not be able to identify suitable acquisition candidates or consummate acquisitions on acceptable terms, or we may be unable to successfully integrate acquisitions, which could disrupt our operations and adversely impact our business and operating results. A component of our growth strategy is to acquire complementary businesses in order to enhance the solutions we offer to our customers. We ~~intend to~~ continue to pursue acquisitions of complementary technologies, products, data sources and businesses as a component of our growth strategy. Acquisitions involve certain known and unknown risks that could cause our actual growth or operating results to differ from our expectations. For example, we may not be able to identify suitable acquisition candidates or to consummate acquisitions on acceptable terms; we may not be able to obtain the necessary financing, on favorable terms or at all, to finance any or all of our potential acquisitions; and acquired technologies, products or businesses may not perform as we expect and we may fail to realize anticipated revenue and profits. In addition, our acquisition strategy may divert management' s attention away from our existing business, resulting in the loss of key customers or employees, and expose us to unanticipated problems or legal liabilities, including responsibility as a successor for undisclosed or contingent liabilities of acquired businesses or assets. If we fail to conduct due diligence on our potential targets effectively, for example, we may not identify problems at target companies or fail to recognize incompatibilities or other obstacles to successful integration. Our inability to successfully integrate future acquisitions could impede us from realizing all of the benefits of those acquisitions and could severely weaken our business operations. The integration process may disrupt our business and, if new technologies, products or businesses are not implemented effectively, may preclude the realization of the full benefits expected by us and could harm our results of operations. In addition, the overall integration of new technologies, products or businesses may result in unanticipated problems, expenses, liabilities and competitive responses. Further, even if the operations of an acquisition are integrated successfully, we may not realize the full benefits of the acquisition, including the synergies, cost savings or growth opportunities that we expect. These benefits may not be achieved within the anticipated time frame, or at all. Further, acquisitions may cause us to issue common stock that would dilute our current stockholders' ownership percentage, use a substantial portion of our cash resources, experience volatility in earnings due to changes in contingent consideration related to acquisition earn- out liability estimates or become subject to litigation. If we do not successfully develop and deploy new products and technologies to address the needs of our customers, our business and results of operations could suffer. Our success is based on our ability to design information products that enable the integration of data into a common operating environment to facilitate advanced data analysis, knowledge management and collaboration. We are also heavily reliant on our information technology infrastructure, processes and procedures and will devote significant resources to ensuring we have competitive

informational technology systems. Information technology changes rapidly, however, and we may not be able to stay ahead of such advances. If we are unable to introduce new or upgraded products, services or technology that users and collaborators recognize as valuable, we may fail to generate additional engagement on our platforms, attract and retain customers or monetize the activity on our platforms. We have spent substantial amounts of time and money researching and developing new technologies and enhanced versions of existing features to meet customers' and potential customers' rapidly evolving needs and our efforts to develop new and upgraded products, services or technology will require us to continue to incur significant costs. We cannot guarantee current or prospective users and customers will respond favorably to new or improved products, services or technology. The introduction of new products and services by competitors or the development of entirely new technologies to replace existing offerings could make our platforms obsolete or adversely affect our business, financial condition and results of operations. We may experience difficulties with software development, design, or marketing that delay or prevent our development, introduction, or implementation of new platforms, features, or capabilities. Any delays could result in adverse publicity, loss of revenue or market acceptance, or claims by customers, any of which could harm our business. Moreover, the design and development of new platforms or new features and capabilities to existing platforms may require substantial investment, and there is no assurance that such investments will be successful. If customers do not widely adopt our new platforms, experiences, features, and capabilities, we may not be able to realize a return on our investment and our business, financial condition, and results of operations may be adversely affected. New and existing platforms and changes to existing platforms could fail to attain sufficient market acceptance for many reasons, including: • the failure to predict market demand accurately in terms of product functionality and to supply offerings that meet this demand in a timely fashion; • product defects, errors or failures or our inability to satisfy customer service level requirements; • negative publicity or negative private statements about the security, performance or effectiveness of our platforms or product enhancements; • delays in releasing to the market new offerings or enhancements to existing offerings; • the introduction or anticipated introduction of competing platforms or functionalities by competitors; • the inability of our platforms or product enhancements to scale and perform to meet customer demands; and • receiving qualified or adverse opinions in connection with security or penetration testing, certifications or audits, such as those related to IT controls and security standards and frameworks or compliance. If we are not able to continue to identify challenges faced by our customers and develop, license or acquire new features and capabilities to our offerings in a timely and cost- effective manner, or if such enhancements do not achieve market acceptance, our business, financial condition, results of operations, and prospects may suffer and anticipated revenue growth may not be achieved. ~~Our business and operations have been and may in the future be adversely affected by the novel coronavirus (COVID- 19) pandemic. The COVID- 19 pandemic, and the various governmental, industry and consumer actions related thereto, had, and may continue to have, an adverse effect on our business, financial condition and results of operations. These effects have included, and may include in the future, a negative impact on the availability of our key personnel, temporary closures of our offices or the facilities of our business partners, customers, suppliers, third party service providers or other vendors, an increased risk of customer defaults or delays in payments or purchasing decisions and the interruption of domestic and global supply chains, distribution channels, liquidity and capital or financial markets. Even after the COVID- 19 pandemic has subsided, we may continue to experience material and adverse impact on our business, operating results and financial condition as a result of its global economic impact, including any recession that has occurred or may occur in the future. The ultimate impact of the COVID- 19 pandemic or a similar health epidemic is highly uncertain and subject to change.~~ We depend on computing infrastructure operated by third parties to support some of our solutions and customers, and any errors, disruption, performance problems, or failure in their or our operational infrastructure could adversely affect our business, financial condition and results of operations. The software, internal applications and systems underlying our products and services are inherently complex and may contain defects or errors, particularly when first introduced or when new versions or enhancements are released. The development, expansion, operation and maintenance of our technology and network infrastructure is expensive and complex and requires significant internal and external resources. If we do not successfully develop, expand, operate or maintain our technology and network infrastructure, or if we experience operational failures, our reputation could be harmed, and we could lose current and prospective customers and service providers, which could adversely impact the business, financial condition or results of operations. We rely on third parties for certain services made available to users of our platforms, which could limit our control over the quality of the user experience and our cost of providing services. Our ability to generate revenue will be affected by the amount of time it takes to complete and enhance our platform. Additionally, there are multiple third- party vendors and service providers that must continue to provide us access to their application programming interfaces and operating systems, and we will rely on cooperation from third parties to integrate with their systems. Should third- party vendors, service providers and collaborators not perform as expected, cooperate with us or deliver their work as planned, we may not be able to release our products and services in a timely manner. We utilize third- party software in our product and service offerings and expect to continue to do so. The correction of these errors and defects will be dependent on these third parties, so it may be difficult for us to correct them. Further, we cannot be certain that third- party licensors will continue to make their software available to us on acceptable terms, or invest the appropriate levels of resources in their software to maintain and enhance our capabilities or remain in business. We may not be able to successfully manage our intellectual property and we may be subject to infringement claims. Part of our success will depend on our ability to protect our proprietary rights in the technologies used in our products. We will consider trade secrets, including confidential and unpatented technology, important to the maintenance of our competitive position. However, trade secrets and know- how are difficult to protect. Further, if any of our trade secrets were to be lawfully obtained or independently developed by a competitor, we would have no right to prevent that competitor from using the technology or information to compete with us. If any of our trade secrets were to be disclosed to or independently developed by a competitor, our competitive position could be materially and adversely harmed. Additionally, if we are unable to protect our proprietary rights adequately, our business could be harmed. There has been substantial litigation in internet and software-

related industries regarding patent, trademark and copyrights and other intellectual property rights and, from time to time, third parties may claim infringement by us of their intellectual property rights. If we were found to be infringing on the intellectual property rights of any third party, we could be subject to liabilities for such infringement, which could have a material adverse impact on our profitability. In addition, any such claims could distract management from conducting the business. Real or perceived errors, failures, defects or bugs in our platforms, products or services could adversely affect our results of operations and growth prospects. Because we offer very complex platforms, products and services, undetected errors, defects, failures or bugs may occur, especially when platforms or capabilities are first introduced or when new versions or other product or infrastructure updates are released. These platforms are often installed and used in large- scale computing environments with different operating systems, software products and equipment, and data source and network configurations, which may cause errors or failures in our platforms or may expose undetected errors, failures, or bugs in our platforms. The platforms often have different versions and updates based off of specific- state requirements. Despite testing, errors, failures, or bugs may not be found in new software or releases until after commencement of commercial shipments. Errors can also delay the development or release of new platforms or capabilities or new versions of platforms, adversely affect our reputation and our customers' willingness to buy our platforms, and adversely affect market acceptance or perception of these platforms. Many customers use these platforms, products and services in applications that are critical to their businesses or missions and may have a lower risk tolerance to defects in our platforms, products and services than to defects in other, less critical, software products. Any errors or delays in releasing new software or new versions of platforms, products and services or allegations of unsatisfactory performance or errors, defects or failures in released software could cause us to lose revenue or market share, increase our service costs, result in substantial costs in redesigning the software, result in the loss of significant customers, subject us to liability for damages and divert company resources from other tasks, any one of which could materially and adversely affect our business, results of operations and financial condition. In addition, our platforms could be perceived to be ineffective for a variety of reasons outside of our control. Hackers or other malicious parties could circumvent our or customers' security measures, and customers may misuse our platforms resulting in a security breach or perceived product failure. Real or perceived errors, failures, or bugs in our platforms, products and services, or dissatisfaction with those services or outcomes, could result in customer terminations and / or claims by customers for losses sustained by them. In such an event, we may be required, or may choose, for customer relations or other reasons, to expend additional resources in order to help correct any such errors, failures, or bugs. In a dynamic industry like ours, our success and growth depend on our ability to attract, recruit, retain and develop qualified employees. Our business functions at the intersection of rapidly changing technological, social, economic and regulatory developments that require a wide- ranging set of expertise and intellectual capital. To continue to successfully compete and grow, we must attract, recruit, develop and retain the necessary personnel who can provide the needed expertise across the entire spectrum of our intellectual capital needs. While we have a number of key personnel who have substantial experience with our operations, we must also develop our personnel to provide succession plans capable of maintaining continuity in the midst of the inevitable unpredictability of human capital. The market for qualified personnel is competitive, and we may not succeed in recruiting additional personnel or may fail to effectively replace current personnel who depart with qualified or effective successors. Our effort to retain and develop personnel may also result in significant additional expenses, which could adversely affect our profitability. There can be no assurances that qualified employees will continue to be employed or that we will be able to attract and retain qualified personnel in the future. Failure to retain or attract key personnel could have a material adverse effect on our business, financial condition and results of operations. We have identified material weaknesses in our internal control over financial reporting which, if not timely remediated, may adversely affect the accuracy and reliability of our financial statements and our reputation, business and stock price, as well as lead to a loss of investor confidence in us. As a public company, we are required to maintain internal control over financial reporting and to report any material weaknesses in such internal control. Section 404 of Sarbanes- Oxley Act of 2002, as amended (the " Sarbanes- Oxley Act "), requires that we furnish a report by management on, among other things, the effectiveness of our internal control over financial reporting. This assessment is required to include disclosure of any material weaknesses identified by our management in our internal control over financial reporting. Our independent registered public accounting firm will not be required to attest to the effectiveness of our internal control over financial reporting until our first annual report required to be filed with the SEC following the later of the date we are deemed to be an " accelerated filer " or a " large accelerated filer, " each as defined in the Securities Exchange Act of 1934, as amended (the " Exchange Act "), or the date we are no longer an " emerging growth company, " as defined in the Jumpstart Our Business Startups Act enacted in April 2012 (" JOBS Act "). If we have a material weakness in our internal control over financial reporting, we may not detect errors on a timely basis and our financial statements may be materially misstated. As described under " Item 9A. Controls and Procedures, " we concluded that our disclosure controls and procedures were not effective as of December 31, ~~2022~~ **2023** , and that we had, as of such date, material weaknesses in our internal control over financial reporting related to ~~(i) the lack of segregation of duties over the cash, accounts payable, payroll, and financial reporting transaction classes; (ii) the lack of evidence of formalization surrounding internal controls and the financial close processes and (iii)~~ the lack of properly designed general information technology controls surrounding logical access, change management, and vendor application management. A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting such that there is a reasonable possibility that a material misstatement of our annual or interim consolidated financial statements would not be prevented or detected on a timely basis. We intend to remediate these material weaknesses. While we believe the steps we take to remediate these material weaknesses will improve the effectiveness of our internal control over financial reporting and will remediate the identified deficiencies, if our remediation efforts are insufficient to address the material weaknesses or we identify additional material weaknesses in our internal control over financial reporting in the future, our ability to analyze, record and report financial information accurately, to prepare our financial statements within the time periods specified by the rules and forms of the SEC and to otherwise comply with our

reporting obligations under the federal securities laws may be adversely affected. The occurrence of, or failure to remediate, these material weaknesses and any future material weaknesses in our internal control over financial reporting may adversely affect the accuracy and reliability of our financial statements and have other consequences that could materially and adversely affect our business, including an adverse impact on the market price of our common stock. In addition, we could become subject to investigations by Nasdaq, the SEC or other regulatory authorities, which could require additional financial and management resources. If our internal control 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. We rely on financial reporting and data analytics that must be accurate in order to make real- time management decisions, accurately manage our cash position, and maintain adequate inventory levels while conserving adequate cash to fund operations. In the event of a systems failure, a process breakdown, the departure of key management or fraud, we would be unable to efficiently manage these items and may experience liquidity shortfalls that our cash position or revolving credit facility may not be able to accommodate. In such a situation, we also 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. We may be unable to accurately forecast our operating results and growth rate, which may adversely affect our reported results and stock price. We may not be able to accurately forecast our operating results and growth rate. We use a variety of factors in our forecasting and planning processes, including historical results, recent history and assessments of economic and market conditions. Our growth rates may not be sustainable, and our growth depends on the continued growth of demand for the products we offer. Lower demand caused by changes in customer preferences, a weakening of the economy or other factors may result in decreased revenues or growth. Furthermore, many of our expenses and investments are fixed, and we may not be able to adjust our spending in a timely manner to compensate for any unexpected shortfall in our operating results. Failure to accurately forecast our operating results and growth rate could cause our actual results to be materially lower than anticipated. If our growth rate declines as a result, investors' perceptions of our business may be adversely affected, and the market price of our common stock could decline. Consolidation in the industries in which our customers operate may reduce the volume of services purchased by consolidated customers following an acquisition or merger, which could materially harm our operating results and financial condition. Mergers or consolidations among our customers could in the future reduce the number of our customers and potential customers. When companies consolidate, overlapping services previously purchased separately are usually purchased only once by the combined entity, leading to loss of revenue. Other services that were previously purchased by one of the merged or consolidated entities may be deemed unnecessary or cancelled. If our customers merge with or are acquired by other entities that are not our customers, or that use fewer of our services, they may discontinue or reduce their use of our services. There can be no assurance as to the degree to which we may be able to address the revenue impact of such consolidation. Any of these developments could materially harm our operating results and financial condition. ~~Adverse developments affecting the financial services industry 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, Silicon Valley Bank (" SVB ") was closed by the California Department of Financial Protection and Innovation, which appointed the Federal Deposit Insurance Corporation (" FDIC ") as receiver. Similarly, on March 12, 2023, Signature Bank and Silvergate Capital Corp. were each swept into receivership. The 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 have no borrowing or deposit exposure to SVB, Signature or Silvergate and have not experienced any adverse impact to our liquidity or to our current and projected business operations, financial condition or results of operations as a result of these recent events. 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 at this time. Additionally, certain of our data suppliers or customers 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 us, 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.~~ Risks Related to Regulatory and Legal Matters **Federal** ~~Our business is subject to complex~~ and ~~evolving U. S. and non- U. S. laws and regulations regarding privacy, data protection and security, technology protection and other matters. Many of these laws and regulations are subject to change and uncertain interpretation and could result in claims, changes to our business practices, monetary penalties, increased cost of operations or otherwise harm our business. We are subject to a variety of local,~~ state ~~, national and international laws and directives and regulations in the United States and abroad that involve matters central to our business, including privacy and data protection, data security, data storage, retention, transfer and deletion, technology protection and personal information. Foreign data protection, data security, privacy and other laws and regulations can impose different obligations or be more restrictive than those in the United States. These U. S. federal and state and foreign laws and regulations, which, depending on the regime, may be enforced by private parties or government entities, are constantly evolving and can be subject to significant change, and they are likely to remain uncertain for the foreseeable future. In addition, the application, interpretation, and enforcement of these laws and regulations are often uncertain and may be interpreted and applied inconsistently from country to country and inconsistently with our current policies and practices. A number of proposals are pending before U. S. federal, state, and foreign legislative and regulatory bodies that could significantly affect our business. The overarching complexity of~~ privacy and data protection laws **are evolving** and ~~regulations around the world pose a compliance challenge that could manifest in costs, damages or liability in other forms as a result of failure to implement proper programmatic controls, failure to adhere to those controls or the malicious~~

~~or inadvertent breach of applicable privacy and data protection requirements by us, our employees, our business partners or our customers. In addition to government regulation, self- regulatory standards and other industry standards may legally or contractually apply to us, be argued to apply to us, or we may elect to comply with such standards or to facilitate our customers'~~ compliance with ~~such standards~~ **applicable requirements may increase our operating costs or adversely impact our ability to service our customers and market our products and services** . ~~Because~~ **Federal and state laws and regulations regarding the collection, retention, security, use, disclosure and transfer of personal data (collectively, " Privacy Laws ") are changing, increasing in number and expanding in scope. Existing Privacy Laws include HIPAA, which regulates protected health information (" PHI ") created or received by or on behalf of health care providers, health plans, and other covered entities. The recently enacted Washington My Health My Data Act gives Washington consumers rights with respect to consumer health data, which is defined expansively. In recent years, several states have adopted Privacy Laws that regulate the** privacy ~~,~~ **and security of personal** data **much more broadly than U. S. laws have in the past. The California Consumer Privacy Act, as amended by the California Privacy Rights Act, the Connecticut Act Concerning Personal Data Privacy and Online Monitoring, the Colorado Privacy Act, the Virginia Consumer Data** ~~protection~~ **Protection Act** and ~~information security~~ **the Utah Consumer Privacy Act all went into effect in 2023. Nine additional states (i. e., Delaware, Florida, Iowa, Indiana, Montana, New Jersey, Oregon, Tennessee and Texas) have passed comprehensive Privacy Laws that will go into effect from 2024 through 2026, and several additional states** are **considering similar laws. It is possible that** ~~critical competitive factors in our industry, we may make statements on our website, in marketing materials or in other settings about our data security measures and our compliance with, or our ability to facilitate our customers' compliance with,~~ these ~~standards. We also expect that there will continue to be new proposed laws and regulations concerning privacy~~ **Privacy** ~~, data protection and information security and we cannot yet determine the impact such future laws~~ **Laws** ~~, regulations and standards, or amendments to or re- interpretations of existing laws and regulations, industry standards, or other obligations may have on our business. New laws, amendments to or re- interpretations of existing laws and regulations, industry standards and contractual and other obligations may require us to incur additional costs and restrict our business operations. As these legal regimes relating to privacy, data protection and information security continue to evolve, they may result in ever- increasing public scrutiny and escalating levels of enforcement and sanctions. Furthermore, because the interpretation and application of laws, standards contractual obligations and other obligations relating to privacy, data protection and information security are uncertain, these laws, standards and contractual and other obligations~~ may be interpreted and applied in a manner that is ~~, or is alleged to be,~~ inconsistent with **our data practices. Establishing and maintaining compliance with these various Privacy Laws could cause us or the third parties that license us data to incur substantial costs or require changes in business practices that are adverse to our business. The products and services we offer include the license of information products that contain data that have been de- identified in accordance with the requirements of applicable Privacy Laws, including HIPAA, and therefore are largely beyond the scope of current Privacy Laws. However, we may receive personal data, including PHI, for purposes of de- identifying such information prior to integrating the de- identified data into the environment that informs our information products. These state Privacy Laws are very recent and thus far there has been little interpretation of these laws by regulators or courts. Accordingly, there is uncertainty as to whether the de- identification requirements under the more recent Privacy Laws conform with the HIPAA de- identification standards. Compliance with state Privacy Laws could require additional investment and management attention and may subject us to significant liabilities if we or our data suppliers do not comply appropriately with new and potentially conflicting laws and regulations. If there is a future change in Privacy Laws, we may also face limitations on our ability to use de- identified information that could harm our business. There is also a risk that the third parties that license us data and de- identification software may fail to properly de- identify PHI under HIPAA or personal data under applicable state Privacy Laws, some of which may impose different standards for de- identification than those required by HIPAA. The privacy, security and breach notification rules promulgated under HIPAA establish a set of national privacy and security standards for the protection of PHI by health plans, health care clearinghouses and certain health care providers, referred to as " covered entities, " and the third parties with which such covered entities contract for services, referred to as " business associates, " that engage in creating, receiving, maintaining or transmitting PHI. While we generally do not consider our products and services to subject us to HIPAA, both because the healthcare data contained within our information products are de- identified to remove PHI before being ingested into our environments and because we do not constitute a covered entity, in certain scenarios, we may nevertheless be contractually obligated to comply with certain HIPAA obligations as a business associate of a covered entity, including the various requirements of the HIPAA de- identification rules. Additionally, if PHI is inadvertently introduced into our environments without being properly de- identified, we may be directly liable for failing to meet the obligations of a business associate under HIPAA. The U. S. Department of Health and Human Services Office for Civil Rights may impose penalties for a failure to comply with applicable requirement of HIPAA. Penalties will vary significantly depending on factors such as the date of the violation, whether the business associate knew or should have known of the failure to comply, or whether the business associate' s failure to comply was due to willful neglect. Mandatory penalties for HIPAA violations can be significant. A single breach incident can result in violations of multiple standards. If a person knowingly or intentionally obtains or discloses PHI in violation of HIPAA requirements, criminal penalties may also be imposed. We have implemented practices and procedures to facilitate our continued compliance with applicable Privacy Laws, which steps include engaging third parties to provide guidance with respect to the de- identification of the data that informs our information products and certification at least annually as to the privacy and security frameworks we have established (e. g., with respect to de- identification under HIPAA and system and organization controls). In addition to our reliance on those third parties, we are dependent on the third parties that**

license us data to deliver information to us in a form and in a manner that complies with applicable Privacy Laws. There is no assurance that the safeguards and controls employed by us or the third parties that license us data and de-identification software will be sufficient to prevent a breach of applicable Privacy Laws, or that claims will not be filed against us or these third parties despite such safeguards and controls. Data suppliers might decide to modify or discontinue their services without adequate notice, which may cause additional expense in arranging new services and could harm our reputation, business, operating results and financial condition. Many Privacy Laws protect more than health- related information, and although they vary by jurisdiction, these laws can extend to employee information, business information, healthcare provider information and other information relating to identifiable individuals. Recently enacted comprehensive state Privacy Laws impose enhanced data privacy obligations for entities that fall within the scope of these laws and create individual privacy rights for residents, including the right to access and delete their personal information, the right to opt- out of certain sharing and sales of their personal information and the right to opt- in to the sharing of sensitive personal information, including information about health and race. These regulations and legislative developments have potentially far- reaching consequences and may require us to modify our data management practices ~~, our policies or procedures or~~ **and to incur substantial expense in order to comply. Failure to comply with** ~~the~~ **these laws may result** ~~features of our solutions. If so,~~ in ~~addition to the possibility of fines~~ , **among** ~~lawsuits, and~~ other ~~claims~~ **things** , **civil and criminal liability, negative publicity, damage to our reputation and liability under contractual provisions. These Privacy Laws may also increase our compliance costs and influence or limit the types of products and services that** we **can provide. The occurrence of any of the foregoing** could ~~be~~ **impact our ability to provide the same level of service to our customers,** ~~required~~ **require us** to ~~fundamentally change our business activities and practices or~~ modify our ~~solutions~~ **offerings or increase our costs** , which could have ~~an~~ **a material** adverse effect on our business **, financial condition** ~~. We may be unable to make such changes~~ and ~~modifications~~ **results of operations. In addition to the increase** in ~~a commercially reasonable manner~~ **states enacting Privacy Laws and the potential** ~~or~~ **for** ~~at all and~~ **the scope of those laws to materially affect our compliance obligations, continued public policy discussions regarding whether the current standards for the de- identification of health information are sufficient to adequately protect individual patient privacy may present potential risks to our business. These discussions may lead to further restrictions on the use of de-identified data. There can be no assurance that these initiatives or future initiatives will not adversely affect** our ability to **continue to license** ~~fulfill existing obligations, make enhancements or develop new solutions and features could be limited. Furthermore, the costs of compliance with, and other~~ -- **the data** ~~burdens imposed by, the laws, regulations and policies~~ that **informs our current and future information offerings. Further, regulatory authorities around the world have enacted and** are **considering a number** ~~applicable to the businesses~~ of **legislative proposals concerning** ~~our customers may limit the use and adoption of, and reduce the overall demand for, our solutions. These existing and proposed laws and regulations can be costly to comply with and can make our solutions and services less effective or valuable, delay or impede the development of new products, result in negative publicity, increase our operating costs, require us to modify our data handling practices, limit our operations, impose substantial fines and penalties, require significant management time and attention, or put our data or technology at risk. Any failure or perceived failure by us or our solutions to comply with U. S. or applicable foreign laws, regulations, directives, policies, industry standards or legal obligations relating to~~ privacy ~~,~~ **and** data protection ~~or information security, or any security incident that results in loss of or the unauthorized access to, or acquisition, use, release, or transfer of, personal information, personal data, or other customer or sensitive data sensitive data or information, may result in governmental investigations, inquiries, enforcement actions and prosecutions, private claims and litigation, indemnification or other contractual obligations, other remedies~~ , including ~~fines~~ **the European Union' s General Data Protection Regulation, the United Kingdom' s Data Protection Act of 2018 and Canada' s Personal Information Protection and Electronic Documents Act. Although** ~~or~~ **our** ~~demands that we modify or cease existing~~ business ~~practices, or adverse publicity, and related costs and liabilities, which could significantly and adversely affect our business and results of operations. Privacy regulation~~ is **not currently subject** ~~an evolving area and compliance with applicable privacy regulations may increase our operating costs or adversely impact our ability~~ to **these global requirements** ~~service our customers and market our products and services. Federal and state governments and agencies have adopted~~ , ~~or are considering adopting,~~ **as we expand we may become subject to the** laws ~~and regulations regarding the collection, use and disclosure~~ of ~~data~~ **additional jurisdictions, domestic and foreign** . It is possible that these laws may be interpreted and applied in a manner that is inconsistent with our data **management** ~~practices, which could cause us to incur additional cost. Moreover, complying with these various laws could cause us to incur substantial costs or require us to change our business practices in a manner adverse to the business. We intend to meet or exceed all applicable regulatory requirements; however, the work of our internal resources in conjunction with third party services may result in the failure to achieve or maintain compliance with such requirements, and our third- party services suppliers might decide to modify or discontinue their services without adequate notice and this might cause additional expense in arranging new services and could harm our reputation, business, operating results and financial condition. Regulatory authorities around the world are considering a number of legislative proposals concerning privacy and data protection. Federal and state governments and agencies have adopted, or are considering adopting, laws and regulations regarding the collection, use and disclosure of data. As our business expands, it may become subject to laws of additional jurisdictions, domestic and foreign. It is possible that these laws may be interpreted and applied in a manner that is inconsistent with our data~~ practices. If so, in addition to the possibility of fines, any increase in the costs of compliance with, and other burdens imposed by, applicable legislative and regulatory initiatives may limit our ability to collect, aggregate or use data **to inform our information products** . Moreover, complying with ~~these~~ various **global Privacy** ~~laws~~ **Laws** could cause us to incur substantial costs or require us to change our business practices in a manner adverse to our business **. Security breaches and unauthorized use of our systems and information could expose us, our customers, our data suppliers or others to risk of loss. We rely on information**

technology systems and networks, and those of third- party vendors, to ensure the continuity of our business operations and to process and store data, including proprietary data, personal data that may be subject to legal protection and de-identified data that may be subject to contractual security obligations. Despite our efforts to protect our systems, cybersecurity threats pose a risk to the security and availability of our systems and networks and the confidentiality, integrity and availability of our data. One or more cyber threats might defeat the measures that we take to anticipate, detect, avoid or mitigate such threats. Certain techniques used to obtain unauthorized access, introduce malicious software, disable or degrade service, or sabotage systems may be designed to remain dormant until a triggering event and we may be unable to anticipate these techniques or implement adequate preventative measures since techniques change frequently or are not recognized until launched, and because cyberattacks can originate from a wide variety of sources. Although we take steps to manage and avoid these risks and to prevent their recurrence, our preventive and remedial actions may not be successful. Such attacks, whether successful or unsuccessful, could result in our incurring costs related to, for example, rebuilding internal systems, defending against litigation, responding to regulatory inquiries or actions, paying damages or fines, or taking other remedial steps with respect to third parties. Publicity about vulnerabilities and attempted or successful incursions could damage our reputation with clients and data suppliers and reduce demand for our services. To the extent that any disruption or security breach results in a loss or damage to our data, an inappropriate disclosure of proprietary or sensitive information, an inability to access data sources, or an inability to process data or provide our offerings to our customers, it could cause significant damage to our reputation, affect our relationships with our data suppliers and customers (including loss of data suppliers and customers), lead to claims against us and ultimately harm our business. We may be required to incur significant costs to alleviate, remedy or protect against damage caused by these disruptions or security breaches in the future. We may also face inquiry or increased scrutiny from government agencies as a result of any such disruption or breach. While we have insurance coverage for certain instances of a cyber security breach, our coverage may not be sufficient if we suffer a significant attack or multiple attacks. Any such breach or disruption could have a material adverse effect on our operating results and our reputation as a service provider. Also, our data suppliers have responsibility for security of their own computer and communications environments. These third parties face risks relating to cyber security similar to ours, which could disrupt their businesses and therefore materially impact ours. Accordingly, we are subject to any flaw in or breaches to their computer and communications systems or those that they operate for us, which could result in a material adverse effect on our business, operations and financial results . If we fail to perform our services in accordance with contractual requirements, regulatory standards and ethical considerations, we could be subject to significant costs or liability and our reputation could be harmed. We maintain and process a large amount of data. This data is often accessed through transmissions over public and private networks, including the internet. Despite our physical security measures, implementation of technical controls and contractual precautions designed to identify, detect and prevent the unauthorized access, alteration, use or disclosure of our data, there is no guarantee that these measures or any other measures can provide absolute security. Systems that access or control access to our services and databases may be compromised as a result of criminal activity, including cyber-attacks and other intentional business disruptions, negligence or otherwise. Unauthorized disclosure or use, or loss or corruption, of our data or inability of our users to access our systems could disrupt the operations, subject us to substantial legal liability, result in a material loss of business, cause us to incur significant cost and significantly harm our reputation. Risks Related to Ownership of our Common ~~Stock~~ **StockThe** ~~The~~ market price of our common stock may be volatile, and holders of our common stock could lose a significant portion of their investment due to drops in the market price of our common stock. The market price of our common stock may be volatile and stockholders may not be able to resell their Forian common stock at or above the price at which they are deemed to have acquired the Forian common stock pursuant to the Business Combination or otherwise due to fluctuations in our market price, including changes in price caused by factors unrelated to our operating performance or prospects. Specific factors that may have a significant effect on the market price for **our** ~~the combined company's~~ common stock include, among others, the following: • changes in stock market analyst recommendations or earnings estimates regarding our common stock, other companies comparable to us or companies in the industries we serve; • actual or anticipated fluctuations in our operating results or future prospects; • reaction to our public announcements; • strategic actions taken by us or our competitors, such as any contemplated business separation, acquisitions or restructurings; • adverse conditions in the financial market or general U. S. or international economic conditions, including those resulting from war, incidents of terrorism and responses to such events; and • sales of common stock by us, members of our management team or significant stockholders. We do not intend to pay dividends on our common stock, so any returns will be limited to the value of our stock. We currently anticipate that we will retain future earnings for the development, operation and expansion of our business and do not anticipate declaring or paying any cash dividends for the foreseeable future. In addition, we may enter into agreements that prohibit us from paying cash dividends without prior written consent from our contracting parties, or which other terms prohibiting or limiting the amount of dividends that may be declared or paid on our common stock. Any return to stockholders will therefore be limited to the appreciation of their stock, which may never occur. The directors and management of Forian ~~will~~ own a significant percentage of our common stock and **are** ~~will be~~ able to exert significant control over matters subject to stockholder approval. Our directors and officers beneficially own approximately ~~43~~ **45** % of our outstanding common stock. These stockholders may be able to determine all matters requiring stockholder approval. For example, these stockholders may be able to control elections of directors, amendments of our organizational documents or approval of any merger, sale of assets or other major corporate transaction. This may prevent or discourage unsolicited acquisition proposals or offers for Forian common stock that you may feel are in your best interest as one of our stockholders. The interests of this group of stockholders may not always coincide with your interests or the interests of other stockholders and they may act in a manner that advances their best interests and not necessarily those of other stockholders, including seeking a premium value for their common stock, and might affect the

prevailing market price for our common stock. Raising additional capital may cause dilution to our existing stockholders, restrict our operations or require us to relinquish rights to our technologies or product candidates. We may seek additional capital through a combination of public and private equity offerings, debt financings, strategic partnerships and alliances and licensing arrangements. To the extent that we raise additional capital through the sale of equity or convertible debt securities, your ownership interest will be diluted, and the terms may include liquidation or other preferences that adversely affect your rights as a stockholder. The incurrence of indebtedness would result in increased fixed payment obligations and could involve certain restrictive covenants, such as limitations on our ability to incur additional debt, limitations on our ability to acquire or license intellectual property rights and other operating restrictions that could adversely impact our ability to conduct our business. If we raise additional funds through strategic partnerships and alliances and licensing arrangements with third parties, we may have to relinquish valuable rights to our technologies or product candidates, or grant licenses on terms unfavorable to us. Sales of a substantial number of shares of our common stock by our existing stockholders in the public market could cause our stock price to fall. If our existing stockholders sell, or indicate an intention to sell, substantial amounts of our common stock in the public market, the trading price of our common stock could decline. Our bylaws contain forum limitations for certain disputes between us and our stockholders that could limit the ability of stockholders to bring claims against us or our directors, officers and employees in jurisdictions preferred by stockholders. 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 is the sole and exclusive forum for (i) any derivative lawsuit brought on our behalf, (ii) any lawsuit against our current or former directors, officers, employees, stockholders or agents asserting a breach of a duty (including any fiduciary duty) owed by any such current or former director, officer, stockholder, employee or agent to us or our stockholders, (iii) any lawsuit asserting a claim against us or any of our current or former director, officer, employee, stockholder or agent arising out of or relating to any provision of the DGCL, our charter or bylaws (each, as in effect from time to time), or (iv) any lawsuit asserting a claim against us or any of our current or former directors, officers, employees, stockholders or agents governed by the internal affairs doctrine of the State of Delaware. The foregoing forum provisions do not apply to suits brought to enforce a duty or liability created by the Securities Act, or the Exchange Act or any other claim for which the federal courts have exclusive jurisdiction. Our bylaws also provide that, unless Forian consents in writing to the selection of an alternative forum, the federal district courts of the United States of America are the sole and exclusive forum for the resolution of any complaint asserting a cause of action arising under the Securities Act. The foregoing forum provisions may prevent or limit a stockholder' s ability to file a lawsuit in a judicial forum that it prefers for disputes with us or our directors, officers, employees, stockholders or agents, which may discourage such lawsuits, make them more difficult or expensive to pursue, and result in outcomes that are less favorable to such stockholders than outcomes that may have been attainable in other jurisdictions, although though stockholders will not be deemed to have waived our compliance with federal securities laws and the rules and regulations thereunder. There is uncertainty as to whether a court would enforce such a forum selection provision as written in connection with claims arising under the Securities Act because Section 22 of the Securities Act creates concurrent jurisdiction for federal and state courts over all such Securities Act claims. In addition, notwithstanding the inclusion of the foregoing forum provisions in the bylaws, courts may find the foregoing forum provisions to be inapplicable or unenforceable in certain cases that the foregoing forum provisions purport to address, including claims brought under the Securities Act. If this were to occur in any particular lawsuit, Forian may incur additional costs associated with resolving such lawsuit in other jurisdictions or resolving lawsuits involving similar claims in multiple jurisdictions, all of which could harm our business, results of operations, and financial condition. We are an emerging growth company and a smaller reporting company, and we cannot be certain if the reduced reporting requirements applicable to emerging growth companies and smaller reporting companies will make our common stock less attractive to investors. We are an emerging growth company, as defined in the JOBS Act. For as long as we continue to be an emerging growth company, we may take advantage of exemptions from various reporting requirements that are applicable to other public companies that are not emerging growth companies, including not being required to comply with the auditor attestation requirements of Section 404 of the Sarbanes- Oxley Act, reduced disclosure obligations regarding executive compensation in this Annual Report on Form 10- K and our periodic reports and proxy statements, and exemptions from the requirements of holding nonbinding advisory votes on executive compensation and stockholder approval of any golden parachute payments not previously approved. We could be an emerging growth company for up to five years, although circumstances could cause us to lose that status earlier. We will remain an emerging growth company until the earlier of (1) the last day of the fiscal year (a) following the fifth anniversary of the closing of the Business Combination, (b) in which we have total annual gross revenue of at least $ 1. 07 billion or (c) in which we are deemed to be a large accelerated filer, which requires the market value of our common stock that is held by non- affiliates to exceed $ 700 million as of the prior June 30th, and (2) the date on which we have issued more than $ 1 billion in non- convertible debt during the prior three- year period. Under the JOBS Act, emerging growth companies can also delay adopting new or revised accounting standards until such time as those standards apply to private companies. We have elected to not " opt out " of this exemption from complying with new or revised accounting standards and, therefore, we will adopt new or revised accounting standards at the time private companies adopt the new or revised accounting standard and will do so until such time that we either (i) irrevocably elect to " opt out " of such extended transition period or (ii) no longer qualify as an emerging growth company. Even after we no longer qualify as an emerging growth company, we may still qualify as a " smaller reporting company, " which would allow us to continue to take advantage of many of the same exemptions from disclosure requirements, including not being required to comply with the auditor attestation requirements of Section 404 of the Sarbanes- Oxley Act and reduced disclosure obligations regarding executive compensation in this Annual Report on Form 10- K and our periodic reports and proxy statements. We cannot predict if investors will find our common stock less attractive because we may rely on these exemptions. If some investors find our common stock less attractive as a result, there may be a less active trading market for our common stock and our stock price may be more volatile. We may be at an increased risk of securities class action

litigation. Historically, securities class action litigation has often been brought against a company following a decline in the market price of its securities. If we were to be sued, it could result in substantial costs and a diversion of management' s attention and resources, which could harm our business. Item 1B. Unresolved Staff Comments