Risk Factors Comparison 2024-05-22 to 2023-05-24 Form: 10-K

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

An investment in our common stock involves a high degree of risk. You should carefully consider the risks described below and the other information in this Annual Report on Form 10- K and in other public filings before making an investment decision. Our business, prospects, financial condition, or operating results could be harmed by any of these risks, as well as other risks not currently known to us or that we currently consider immaterial. If any of such risks and uncertainties actually occurs, our business, financial condition or operating results could differ materially from the plans, projections and other forward- looking statements included in the section titled " Management' s Discussion and Analysis of Financial Condition and Results of Operations " and elsewhere in this report and in our other public filings. The trading price of our common stock could decline due to any of these risks, and, as a result, you may lose all or part of your investment. Risks Related to Our Business and Strategy We are dependent upon customer renewals, the addition of new customers and increased revenue from existing customers for our subscription revenue through our LiveRamp platform and our Marketplace and Other business. To sustain or increase our revenue, we must regularly add new ~~clients~~ **customers** and encourage existing ~~clients~~ **customers** to maintain or increase their business with us. As the market matures **and regulation increases,** and as existing and new market participants produce new and different approaches to enable businesses to address their respective needs that compete with our offerings, we may be forced to reduce the prices we charge, may be unable to renew existing customer agreements, or enter into new customer agreements at the same prices and upon the same terms that we have historically obtained. If our new business and cross- selling efforts are unsuccessful or if our customers do not expand their use of our platform or adopt additional offerings and features, our operating results may suffer. Our existing customers have no obligation to renew their contracts upon expiration of their contractual subscription period and may not choose to renew their contracts for a variety of reasons. In the normal course of business, some customers have elected not to renew, and it is difficult to predict attrition rates. Our renewal rates may decline or fluctuate as a result of a number of factors, including customer satisfaction, pricing changes, the prices of services offered by our competitors, mergers and acquisitions affecting our customer base **, regulatory changes such as in privacy, antitrust, or international relations** , and reductions in our customers' spending levels or other declines in customer activity. If our customers do not renew their contracts or decrease the amount they spend with us, our revenue would decline and our business would suffer. A decline in new or renewed subscriptions in any period may not be immediately reflected in our reported financial results for that period but may result in a decline in our revenue in future periods. If we were to experience significant downturns in subscription sales and renewal rates, our reported financial results might not reflect such downturns until future periods. Moreover, the conditions caused by other ~~events~~ **factors** outside our control, such as ~~the COVID- 19 pandemic~~ **macroeconomic growth and increasing global geopolitical tensions** , have affected, and may ~~continue to~~ affect **, directly or indirectly** , the rate of spending on advertising products and have and could continue to adversely affect our customers' ability or willingness to purchase our offerings, delay prospective customers' purchasing decisions, increase pressure for pricing discounts, lengthen payment terms, reduce the value or duration of their subscription contracts, or increase customer attrition rates, all of which could adversely affect our future sales, operating results and overall financial performance. The loss of a contract upon which we rely for a significant portion of our revenues could adversely affect our operating results. Our ten largest ~~clients~~ **customers** represented approximately ~~29~~ **27** % of our revenues in fiscal year ~~2023~~ **2024** ~~. If all of our individual client contractual relationships were aggregated at the holding company level, one client, The Interpublic Group of Companies, accounted for 12 % of our revenues in fiscal year 2023~~ . The loss of, or decrease in revenue from, any of our significant ~~clients~~ **customers** for any reason could have a material adverse effect on our revenue and operating results, which could be exacerbated by ~~client~~ **customer** consolidation, changes in technologies or solutions used by our ~~clients~~ **customers** , changes in demand for our platform, legal or regulatory changes, market optics, ~~client~~ **customer** bankruptcies or departures from their respective industries, pricing **or product** competition **,** or deviation from marketing and sales methods, any one of which may result in even fewer contractual relationships accounting for a high percentage of our revenue and reduced demand from any single significant ~~client~~ **customer** . In addition, some of our ~~clients~~ **customers** have used, and may in the future use, the size and relative importance of their purchases to our business to require that we enter into agreements with more favorable terms than we would otherwise agree to, to obtain price concessions, or to otherwise restrict our business. Data suppliers may withdraw data that we have previously collected or withhold data from us in the future, leading to our inability to provide products and services to our ~~clients~~ **customers** , which could lead to a decrease in revenue and loss of ~~client~~ **customer** confidence. Much of the data that we use is either purchased or licensed from third- party data suppliers, and we are dependent upon our ability to obtain necessary data licenses on commercially reasonable terms. We could suffer material adverse consequences if our data suppliers were to withhold their data from us or materially limit our use of their data, which could occur for a variety of reasons, including because we fail to maintain sufficient relationships with the suppliers or because they decline to provide, or are prohibited from providing, such data to us due to legal, regulatory, contractual, privacy, competitive or other economic concerns. For example, data suppliers could withhold their data from us if there is a competitive reason to do so, if we breach our contract with a supplier, if we breach their expectations of our use of their data, if they are acquired by one of our competitors, if legislation is passed or regulations are adopted restricting or making too difficult the collection, use or dissemination of the data they provide, if market optics become negative regarding the sharing of their data with third parties or allowing the setting of cookies from their sites, if publishers change their privacy policies or user settings, including as a result of legal or regulatory actions, in a material manner that turns off or diminishes the volume of data we receive, or if judicial interpretations are issued

restricting use of such data, or for other reasons. Further, definitions in enacted or proposed state- level data broker legislation apply to LiveRamp, potentially exposing the Company to negative perceptions and diminishing data available to it. Additionally, we could terminate relationships with our data suppliers if they fail to adhere to our data quality standards **or their legal and / or other contractual commitments** . If a substantial number of data suppliers were to withdraw or withhold their data from us or substantially limit our use of their data, or if we were to sever ties with our data suppliers based on their inability to meet appropriate data standards, our ability to provide products and services to our ~~clients~~ **customers** could be materially adversely impacted, which could result in decreased revenues and operating results. Our business is subject to substantial competition from a diverse group of competitors. New products and pricing strategies introduced by these competitors could decrease our market share or cause us to lower our prices in a manner that reduces our revenues and operating margin. We operate in a highly competitive and rapidly changing industry. With the introduction of new technologies and the influx of new entrants to the market, we expect competition to persist and intensify in the future, which could harm our ability to increase revenue and operating results. In addition to existing competitors and intermediaries, we may also face competition from new companies entering the market, which may include large established companies, all of which currently offer, or may in the future offer, products and services that result in additional competition. These competitors may be in a better position to develop new products and pricing strategies that more quickly and effectively respond to changes in customer requirements in these markets. These competitors and new products and technologies may be disruptive to our existing platform offerings, resulting in operating inefficiencies and increased competitive pressure. Some of our competitors may choose to sell products or services competitive to ours at lower prices by accepting lower margins and profitability, or may be able to sell products or services competitive to ours at lower prices given proprietary ownership of data, technical superiority or economies of scale. Such introduction of competent, competitive products, pricing strategies or other technologies by our competitors that are superior to or that achieve greater market acceptance than our products and services could adversely affect our business. In such event, we could experience a decline in market share and revenues and be forced to reduce our prices, resulting in lower profit margins for the Company. Public health emergencies, such as the..... the value of our common stock. The failure to attract, recruit, onboard and retain qualified personnel could hinder our ability to successfully execute our business strategy, which could have a material adverse effect on our financial position and operating results. Our growth strategy and future success depends in large part on our ability to attract, recruit, onboard, motivate and retain technical, ~~client~~ **customer** services, sales, consulting, research and development, marketing, administrative and management personnel ~~, all of which was made more difficult by the COVID- 19 pandemic and the restrictions intended to prevent its spread~~ . The complexity of our products, processing functionality, software systems and services requires highly trained professionals. While we presently have a sophisticated, dedicated and experienced team of executives and employees who have a deep understanding of our business, the labor market for these individuals has historically been very competitive due to the limited number of people available with the necessary technical skills and understanding. As our industry continues to become more technologically advanced, we anticipate increased competition for qualified personnel. In addition, many of the companies with which we compete for experienced personnel may be able to offer greater compensation and benefits packages and / or more flexible work alternatives. We may incur significant costs to attract and retain highly trained personnel and we may lose new employees to our competitors or other technology companies before we realize the benefit of our investment in recruiting and training them, and our succession plans may be insufficient to ensure business continuity if we are unable to retain key personnel. Further, volatility or lack of appreciation in our stock price may also affect our ability to attract and retain our key employees. The loss or prolonged absence of the services of highly trained personnel like our current team of executives and employees, or the inability to recruit, attract, onboard and retain additional, qualified employees, could have a material adverse effect on our business, financial position or operating results. In addition, effective succession planning is important to our long- term success. If we do not develop effective succession planning, the loss of one or more of our key executive or employees or groups of executives or employees could seriously harm our business. ~~In November 2022, we announced (i) a reduction in force involving approximately 10 % of our full- time employees, and (ii) a planned downsizing of our real estate footprint in addition to the footprint reduction which occurred during our fiscal year second quarter. The headcount reduction is part of a broader strategic reprioritization to build a stronger, more profitable company by tightening our focus and simplifying and driving efficiency into our business processes. This reduction, or any location strategy or similar actions taken in the future, could negatively impact our ability to attract, integrate, retain and motivate key executives and employees.~~ If we cannot maintain our culture as we grow, we could lose the innovation, teamwork, passion and focus on execution that we believe contribute to our success, and our business may be harmed. We believe that a critical component to our success has been our company culture, which is based on transparency and personal autonomy. We have invested substantial time and resources in building our team within this company culture. Any failure to preserve our culture could negatively affect our ability to retain and recruit personnel and to proactively focus on and pursue our corporate objectives. **The** ~~Although we have recently reopened our offices and hold in- person meetings and events in compliance with applicable government orders and guidelines, the~~ majority of our employees continue to work remotely. **We** ~~Further, upon the reopening of our offices, we~~ have offered most of our employees the flexibility to determine the amount of time they work in the office, which may present operational challenges and risks, including negative employee morale and productivity, low employee retention, and increased compliance and tax obligations in a number of jurisdictions. If we fail to maintain our company culture, our business may be adversely impacted. Failure to keep up with rapidly changing technologies and marketing practices could cause our products and services to become less competitive or obsolete, which could result in loss of market share and decreased revenues, thereby impacting our results of operations. Advances in information technology are changing the way our ~~clients~~ **customers** use and purchase information products and services and may be disruptive to our existing platform offerings. Maintaining the technological competitiveness of our products, processing functionality, software systems and services is key to our continued success. However, the complexity and uncertainty regarding the development of new technologies and the extent

and timing of market acceptance of innovative products and services create difficulties in maintaining this competitiveness. Without the timely introduction of new products, services and enhancements **that comply with changing laws and standards**, including through the use of new and emerging technologies (e. g., artificial intelligence and machine learning), we could be at a competitive disadvantage and our offerings will become technologically or commercially obsolete over time, in which case our revenue and operating results would suffer. Consumer needs and expectations and the business information industry as a whole are in a constant state of change. Our ability to continually improve our current processes and products in response to changes in technology and to develop new products and services are essential in maintaining our competitive position, preserving our market share and meeting the increasingly sophisticated requirements of our ~~clients~~ **customers**. If we fail to enhance our current products and services or fail to develop new products in light of emerging technologies ~~and~~ **,** industry standards **, and regulations**, we could lose ~~clients~~ **customers** to current or future competitors, which could result in impairment of our growth prospects, loss of market share and decreased revenues. Acquisition and divestiture activities may disrupt our ongoing business and may involve increased expenses, and we may not realize the financial and strategic goals contemplated at the time of a transaction, all of which could adversely affect our business and growth prospects. Historically, we have engaged in acquisitions to grow our business **, such as the acquisition of Habu in January 2024**. To the extent we find suitable and attractive acquisition candidates and business opportunities in the future, we may continue to acquire other complementary businesses, products and technologies and enter into joint ventures or similar strategic relationships. The pursuit of acquisitions may divert the attention of management, disrupt ongoing business, and cause us to incur various expenses in identifying, investigating, and pursuing suitable acquisitions, whether or not they are consummated. While we believe we will be able to successfully integrate newly acquired businesses **(such as Habu)** into our existing operations, there is no certainty that future acquisitions or alliances will be consummated on acceptable terms or that we will be able to successfully integrate the services, content, products and personnel of any such transaction into our operations. In addition, the pursuit of any future acquisitions, joint ventures or similar relationships may cause a disruption in our ongoing business and distract our management and cause us to incur various expenses in identifying, investigating, and pursuing suitable acquisitions, whether or not they are consummated. An acquisition may later be found to have a material legal or ethical issue that was not disclosed or discovered prior to acquisition. Further, we may be unable to realize the revenue improvements, cost savings and other intended benefits of any such transaction. The occurrence of any of these events could result in decreased revenues, net income and earnings per share. We have also divested assets in the past and may do so again in the future. As with acquisitions, divestitures involve significant risks and uncertainties, such as disruption of our ongoing business, reductions of our revenues or earnings per share, unanticipated liabilities, legal risks and costs, the potential loss of key personnel, distraction of management from our ongoing business, and impairment of relationships with employees and ~~clients~~ **customers** because of migrating a business to new owners. Because acquisitions and divestitures are inherently risky, transactions we undertake may not be successful and may have a material adverse effect on our business, results of operations, financial condition or cash flows. Our operations outside the United States are subject to risks that may harm the Company' s business, financial condition or results of operations. During the last fiscal year, we received approximately ~~7~~ **6** % of our revenues from business outside the United States. In those non- U. S. locations where legislation restricting the collection and use of personal data currently exists, less data is available and at a much higher cost. In some foreign markets, the types of products and services we offer have not been generally available and thus are not fully understood by prospective ~~clients~~ **customers**. Upon entering these markets, we must educate and condition the markets, increasing the cost and difficulty of successfully executing our business plan in these markets. Additionally, each of our foreign locations is generally expected to fund its own operations and cash flows, although periodically funds may be loaned or invested from the United States to the foreign subsidiaries. Because of such loans or investments, exchange rate movements of foreign currencies may have an impact on our future costs of, or future cash flows from, foreign investments. We have not entered into any foreign currency forward exchange contracts or other derivative instruments to hedge the effects of adverse fluctuations in foreign currency exchange rates. Additional risks inherent in our non- U. S. business activities generally include, among others, the costs and difficulties of managing international operations, potentially adverse tax consequences, and greater difficulty enforcing intellectual property rights. The various risks that are inherent in doing business in the United States are also generally applicable to doing business outside of the United States, but such risks may be exaggerated by factors normally associated with international operations, such as differences in culture, laws and regulations, especially restrictions on collection, management, aggregation, localizations, and use of information. Failure to effectively manage the risks facing our non- U. S. business activities could materially adversely affect our operating results. Also, our business is subject to weak international economic conditions, geopolitical developments, such as existing and potential trade wars, and other events outside of our control that could result in a reduced volume of business by our customers and prospective customers, and the demand for, and use of, our products and services may decline. For example, the military ~~conflict~~ **conflicts** ~~between Russia~~ **in Europe** and ~~Ukraine~~ **the Middle East** could result in regional instability and adversely impact financial markets as well as economic conditions ~~, especially in Europe~~. In addition, when operating in foreign jurisdictions, we must comply with complex foreign and U. S. laws and regulations, such as the U. S. Foreign Corrupt Practices Act, the U. K. Bribery Act and other local laws prohibiting corrupt payments to government officials, as well as anti- competition regulations and data protection laws and regulations. Violations of these laws and regulations could result in fines and penalties, criminal sanctions, **and** restrictions on our business conduct and on our ability to offer our products and services in one or more countries. Such violations could also adversely affect our reputation with existing and prospective ~~clients~~ **customers**, which could negatively impact our operating results and growth prospects **.Public health emergencies** ~~as the COVID- 19 pandemic,~~ may result in global,national and / or regional economic uncertainty,and measures taken in response to such emergencies could impact our business and future results of operations and financial condition.The COVID- 19 pandemic disrupted the flow of the economy and put unprecedented strains on governments,health care systems,educational institutions,businesses and individuals around the world,and future public health

emergencies could result in the same.Similar to the COVID- 19 pandemic,future public health emergencies could result in significant disruptions to the global financial markets and economic uncertainty,as well as regional quarantines,labor shortages or stoppages,changes in consumer purchasing patterns,disruptions to service providers to deliver data on a timely basis,or at all,and overall economic instability.Any future public health emergencies could materially and adversely affect our business,our operating results,financial condition and prospects,and the value of **our common stock** . A significant breach of the confidentiality of the information we hold or of the security of our or our customers', suppliers', or other partners' computer systems could be detrimental to our business, reputation and results of operations. Our business requires the storage, transmission and utilization of data, including personally identifiable information, much of which must be maintained on a confidential basis. These activities may make us a target of cyberattacks from malicious third parties seeking unauthorized access to the data we maintain, including our data and ~~client~~ **customer** data, or to disrupt our ability to provide service. Any failure to prevent or mitigate security breaches and improper access to or disclosure of the data we maintain, including personal information, could result in the loss or misuse of such data, which could harm our business and reputation and diminish our competitive position. Our ~~clients~~ **customers** and suppliers are increasingly imposing more rigorous contractual obligations on us relating to data security protections. If we are unable to maintain protections and processes at a level equal to that required by our ~~clients~~ **customers** and suppliers, it could negatively affect our relationships with those ~~clients~~ **customers** and suppliers or increase our operating costs. In addition, computer malware, viruses, social engineering, ransomware, phishing and general hacking have become more prevalent, and events outside of our control, such as the military ~~conflict~~ **conflicts** ~~between Russia~~ **in Europe** and ~~Ukraine~~ **the Middle East** , could result in a further increase in such activities. As a result of the types and volume of personal data on our systems, we believe that we are a particularly attractive target for such breaches and attacks. In recent years, the frequency, severity and sophistication of cyberattacks, computer malware, viruses, social engineering, ransomware, phishing and other intentional misconduct by computer hackers have significantly increased, including the ability to evade detection or obscure their activities, and government agencies and security experts have warned about the growing risks of hackers, cyber criminals and other potential attackers targeting information technology systems. Such third parties could attempt to gain entry to our systems for the purpose of stealing data or disrupting the systems. In addition, our security measures may also be breached due to employee error, malfeasance, system errors or vulnerabilities, including vulnerabilities of our vendors, suppliers, their products, or otherwise. Third parties may also attempt to fraudulently induce employees or ~~clients~~ **customers** into disclosing sensitive information such as usernames, passwords or other information to gain access to our ~~clients~~ **customers** ' data or our data, including intellectual property and other confidential business information. The COVID- 19 pandemic generally increased opportunities available to hackers and cyber criminals as more companies and individuals work online from remote locations. We believe we have taken appropriate measures to protect our systems from intrusion, but we cannot be certain that advances in criminal capabilities, discovery of new or existing vulnerabilities in our systems and attempts to exploit those vulnerabilities, physical system or facility break- ins and data thefts or other developments will not compromise or breach the technology protecting our systems and the information we possess. Although we have developed systems and processes that are designed to protect our data, our ~~client~~ **customer** data, and data transmissions to prevent data loss, and to prevent or detect security breaches, our databases ~~have in the past been and in the future~~ may be subject to unauthorized access by third parties, and we may incur significant costs in protecting against or remediating cyberattacks. Any security breach could result in operational disruptions that impair our ability to meet our ~~clients~~ **customers** ' requirements, which could result in decreased revenues. Also, whether there is an actual or a perceived breach of our security, our reputation could suffer ~~irreparable~~ **significant** harm, causing our current and prospective ~~clients~~ **customers** to reject our products and services in the future and deterring data suppliers from supplying us data. Further, we could be forced to expend significant resources in response to a security breach, including those expended in repairing system damage, increasing ~~cyber security~~ **cybersecurity** protection costs by deploying additional personnel and protection technologies, and litigating and resolving legal claims or governmental inquiries and investigations, all of which could divert the attention of our management and key personnel away from our business operations. In any event, a significant security breach could materially harm our business, financial condition and operating results. Our ~~clients~~ **customers** , suppliers and other partners are primarily responsible for the security of their information technology environments, and we rely heavily on them and other third parties to supply clean data content and / or to utilize our products and services in a secure manner. Each of these third parties may face risks relating to ~~cyber security~~ **cybersecurity** , which could disrupt their businesses and therefore materially impact ours. While we provide guidance and specific requirements in some cases, we do not directly control any of such parties' ~~cyber security~~ **cybersecurity** operations, or the amount of investment they place in guarding against ~~cyber security~~ **cybersecurity** threats. Accordingly, we are subject to any flaw in or breaches of their systems, which could materially impact our business, operations and financial results. Finally, while we maintain cyber liability insurance coverage that may cover certain liabilities in connection with a ~~cyber security~~ **cybersecurity** incident, we cannot be certain that our insurance coverage will be adequate for liabilities actually incurred, that insurance will continue to be available to us on commercially reasonable terms, or at all, or that any insurer will not deny coverage as to any future claim. The successful assertion of one or more large claims against us that exceed available insurance coverage, or the occurrence of changes in our insurance policies, including premium increases or the imposition of large deductible or co- insurance requirements, could have a material adverse effect on our business, financial condition, financial results and reputation. Unfavorable publicity and negative public perception about our industry could adversely affect our business and operating results. With the growth of online advertising and e- commerce, there is increasing awareness and concern among the general public, privacy advocates, mainstream media, governmental bodies and others regarding marketing, advertising, and data privacy matters, particularly as they relate to individual privacy interests and the global reach of the online marketplace. Any unfavorable publicity or negative public perception about us, our industry, including our competitors, or even other data- focused industries can affect our business and results of operations, and may lead to digital publishers changing their

business practices or additional regulatory scrutiny or lawmaking that affects us or our industry. For example, in recent years, consumer advocates, mainstream media, elected officials and government officials have increasingly and publicly criticized the data and marketing industry for its collection, storage and use of personal data. Additional public scrutiny may lead to general distrust of our industry, consumer reluctance to share and permit use of personal data and increased consumer opt- out rates, any of which could negatively influence, change or reduce our current and prospective ~~clients~~ **customers** ' demand for our products and services and adversely affect our business and operating results. Interruptions or delays in service from our third- party data center providers could impair our ability to deliver our products and services to our customers, resulting in customer dissatisfaction, damage to our reputation, loss of customers, limited growth and reduction in revenue. We currently serve the majority of our platform functions from third- party data center hosting facilities operated by Google Cloud Platform and Amazon Web Services. Our operations depend, in part, on our third- party facility providers' abilities to protect these facilities against any damage or interruption from natural disasters, such as earthquakes and hurricanes, power or telecommunication failures, criminal acts and similar events. In the event that any of our third- party facilities arrangements ~~is~~ **are** terminated, or if there is a lapse of service or damage to a facility, we could experience interruptions in our platform as well as delays and additional expenses in arranging new facilities and services. Any damage to, or failure of, the systems of our third- party providers could result in interruptions to our platform. Despite precautions taken at our data centers, the occurrence of spikes in usage volume, a natural disaster, such as earthquakes or ~~hurricane~~ **hurricanes** , an act of terrorism, destruction, vandalism or sabotage, a decision to close a facility without adequate notice, or other unanticipated problems at a facility could result in lengthy interruptions in the availability of our platform. Even with current and planned disaster recovery arrangements, our business could be harmed, and ~~there is~~ no assurance can be provided that any interruptions would be remediated without significant cost or in a timely manner or at all. Also, in the event of damage or interruption, our insurance policies may not adequately compensate us for any losses that we may incur. These factors in turn could further reduce our revenue, subject us to liability and cause us to issue credits or cause customers to fail to renew their subscriptions, any of which could materially adversely affect our business. We are dependent on the continued availability of third- party data hosting and transmission services. We incur significant costs with our third- party data hosting services. If the costs for such services increase due to vendor consolidation, regulation, contract renegotiation, or otherwise, we may not be able to increase the fees for our products and services to cover the changes. As a result, our operating results may be significantly worse than forecasted. As the use of " third- party cookies " or other tracking technology continues to be pressured by Internet users, restricted or otherwise subject to unfavorable regulation, blocked or limited by technical changes on end users' devices, or our and our ~~clients~~ **customers** ' ability to use data on our platform is otherwise restricted, our business could be materially impacted. Digital advertising mostly relies on the use of cookies, pixels and other similar technology, including mobile device identifiers that are provided by mobile operating systems for advertising purposes, which we refer to collectively as cookies, to collect data about interactions with users and devices. We utilize third- party cookies, which are cookies owned and used by parties other than the owners of the website visited by the Internet user. Our cookies are used to record information tied to a random unique identifier, including such information as when an Internet user views an ad, clicks on an ad or visits one of our advertiser' s websites through a browser while the cookie is active. We use cookies to help us achieve our advertisers' campaign goals on the web, to limit the instances that an Internet user sees the same advertisement, to report information to our advertisers regarding the performance of their advertising campaigns and to detect and prevent malicious behavior and invalid traffic throughout our network of inventory. Additionally, our ~~clients~~ **customers** use cookies and other technologies to add information they have collected or acquired about users into our platform. Without such data, our ~~clients~~ **customers** may not have sufficient insight into an Internet user' s activity, which may compromise their ability to determine which inventory to purchase for a specific campaign and undermine the effectiveness of our platform. Cookies may be deleted or blocked by Internet users who do not want information to be collected about them. The most commonly used Internet browsers — Chrome, Firefox, Internet Explorer and Safari — allow Internet users to modify their browser settings to prevent cookies from being accepted by their browsers. In May 2023, Google announced it will continue with its previously announced timeline to end Chrome' s support for third ~~-~~ party cookies in the second half of 2024 **and in January 2024 started deprecating third- party cookies for 1 % of its users globally. In April 2024, Google announced a delay to the end of Chrome' s support for third- party cookies, noting it now expects deprecation to be completed in early 2025** . Mobile devices allow users to opt out of the use of mobile device IDs for targeted advertising. Additionally, the Safari browser currently blocks some third- party cookies by default and has recently added controls that algorithmically block or limit some cookies. Other browsers have added similar controls. In addition, Internet users can delete cookies from their computers at any time. Some Internet users also download free or paid ad blocking software that not only prevents third- party cookies from being stored on a user' s computer, but also blocks all interaction with a third- party ad server. Google has introduced ad blocking software in its Chrome web browser that will block certain ads based on quality standards established under a multi- stakeholder coalition. Additionally, the DAA, NAI, their international counterparts, and our company have certain opt- out mechanisms for users to opt out of the collection of their information via cookies. If more Internet users adopt these settings or delete their cookies more frequently than they currently do, or restrictions are imposed by advertisers and publishers, there are changes in technology or new developments in laws, regulations or industry standards around cookies, our business could be harmed. For in- app advertising, data regarding interactions between users and devices are tracked mostly through stable, pseudonymous mobile device identifiers that are built into the device operating system with privacy controls that allow users to express a preference with respect to data collection for advertising, including to disable the identifier. These identifiers and privacy controls are defined by the developers of the mobile platforms and could be changed by the mobile platforms in a way that may negatively impact our business. Privacy aspects of other channels for programmatic advertising, such as CTVs or over- the- top video, are still developing. Technical or policy changes, including regulation or industry self- regulation, could harm our growth in those channels. As the collection and use of data for digital advertising has

received ongoing media attention over the past several years, some government regulators, such as the FTC, and privacy advocates have raised significant concerns around observed data. There has been an array of' do- not- track' efforts, suggestions and technologies introduced to address these concerns, and state statutes are beginning to incorporate the obligation to honor them. However, the potential regulatory and self- regulatory landscape is inherently uncertain, and there is not yet a consensus definition of tracking, nor agreement on what would be covered by' do- not- track' functionality. There is activity by the major Internet browsers to default set on' do- not- track' functionality, including by Safari and Firefox. It is not clear how many other Internet browsers will follow. Substantial increases in the rate and number of people opting out of various data collection processes could have a negative impact on our business and the ecosystems in which we operate. In addition, in the EU, Directive 2002 / 58 / EC (as amended by Directive 2009 / 136 / EC), commonly referred to as the ePrivacy or Cookie Directive, directs EU member states to ensure that accessing information on an Internet user' s computer, such as through a cookie and other similar technologies, is allowed only if the Internet user has been informed about such access and given his or her consent. A replacement for the Cookie Directive to complement and bring electronic communication services in line with the GDPR and force a harmonized approach across EU member states is currently with the EU Council for a trilogue to decide its final effective date. Like the GDPR, the proposed ePrivacy Regulation has extra- territorial application as it applies to businesses established outside the EU who provide publicly available electronic communications services to, or gather data from the devices of, users in the EU. Though still subject to debate, the proposed ePrivacy Regulation may limit the lawful bases available to process digital data collected through cookies and require" opt- in" consent. The fines and penalties for breach of the proposed ePrivacy Regulation may be significant. Limitations on the use or effectiveness of cookies, or other limitations on our, or our ~~clients~~ **customers** ', ability to collect and use data for advertising, whether imposed by EU member state implementations of the Cookie Directive, by the new ePrivacy Regulation, or otherwise, may impact the performance of our platform. We may be required to, or otherwise may determine that it is advisable to, make significant changes in our business operations and product and services to obtain user opt- in for cookies and use of cookie data, or develop or obtain additional tools and technologies to compensate for a lack of cookie data. We may not be able to make the necessary changes in our business operations and products and services to obtain user opt- in for cookies and use of cookie data, or develop, implement or acquire additional tools that compensate for a lack of cookie data. Moreover, even if we are able to do so, such additional products and tools may be subject to further regulation, time consuming to develop or costly to obtain, and less effective than our current use of cookies. ~~Finally, Google, the owner of the Chrome browser, has publicly stated that over the next several years it will no longer support the setting of third- party cookies. Apple, the owner of the Safari browser, had previously ceased supporting third- party cookies. Separately, and combined, these actions will have significant impacts on the digital advertising and marketing ecosystems in which we operate and could negatively impact our business. We are currently offering and continuing to develop non- cookie based alternatives that can be used in the global ecosystem.~~ Climate change may have an impact on our business Any of our primary locations may be vulnerable to the adverse effects of climate change. For example, our offices and facilities in California have experienced, and are projected to continue to experience, climate- related events at an increasing frequency, including drought, water scarcity, heat waves, wildfires and resultant air quality impacts and power shutoffs associated with wildfire prevention. Furthermore, it may be more difficult to mitigate the impact of these events on our remote employees working from home. Changing market dynamics, global policy developments and the increasing frequency and impact of extreme weather events on critical infrastructure in the U. S. and elsewhere have the potential to disrupt our business, the business of our third- party suppliers and the business of our customers, and may cause us to experience higher churn, losses and additional costs to maintain or resume operations. Risks Related to Government Regulation and Taxation Changes in legislative, judicial, regulatory, or cultural environments relating to information collection and use may limit our ability to collect and use data. Such developments could cause revenues to decline, increase the cost and availability of data and adversely affect the demand for our products and services. We receive, store and process personal information and other data from and about consumers in addition to our ~~clients~~ **customers** , employees, and services providers. Our handling of this data is subject to a variety of federal, state, and foreign laws and regulations and is subject to regulation by various government authorities. Our data handling also is subject to contractual obligations and may be deemed to be subject to industry standards. The U. S. federal and various state and foreign governments have adopted or proposed limitations on the collection, distribution, use and storage of data relating to individuals, including the use of contact information and other data for marketing, advertising and other communications with individuals and businesses. In the U. S., various laws and regulations apply to the collection, processing, disclosure, and security of certain types of data. Additionally, the FTC and many state attorneys general are interpreting federal and state consumer protection laws as imposing standards for the online collection, use, dissemination and security of data. In addition, the European Union has been developing new requirements related to the use of data, including in the Digital Services Act, that may impose additional rules and restrictions on the use of the data. The regulatory framework for data privacy issues worldwide is currently evolving and is likely to remain uncertain for the foreseeable future. For example, in the U. S., in August 2022 the FTC released an advance notice of proposed rulemaking concerning commercial surveillance and data security and **sought** ~~is seeking~~ comment on whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies (1) collect, aggregate, protect, use, analyze, and retain consumer data, as well as (2) transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive. In addition, a potential federal data privacy law remains the subject of active discussion, and, in ~~June~~ **April** ~~2022~~ **2024** , a bipartisan ~~group~~ **pair** of lawmakers ~~introduced~~ **unveiled** a **draft** bill that would substantially impact ~~on~~ the online advertising ecosystem if passed. The occurrence of unanticipated events often rapidly drives the adoption of legislation or regulation affecting the use, collection or other processing of data and manners in which we conduct our business. Restrictions could be placed upon the collection, management, aggregation and use of information, which could result in a material increase in the cost of collecting or otherwise obtaining certain kinds of data and could limit the ways in which we may use or disclose information. In particular, interest-

based advertising, or the use of data to draw inferences about a user' s interests and deliver relevant advertising to that user, and similar or related practices, such as cross- device data collection and aggregation, steps taken to de- identify or pseudonymize personal data and to use and distribute the resulting data, including for purposes of personalization and the targeting of advertisements, have come under increasing scrutiny by legislative, regulatory, and self- regulatory bodies in the U. S. and abroad that focus on consumer protection or data privacy. Much of this scrutiny has focused on the use of cookies and other technology to collect information about Internet users' online browsing activity on web browsers, mobile devices, and other devices, to associate such data with user or device identifiers or pseudonymous identifiers across devices and channels. In addition, providers of Internet browsers have engaged in, or announced plans to continue or expand, efforts to provide increased visibility into, and certain controls over, cookies and similar technologies and the data collected using such technologies. For example, in January 2020 Google announced that at some point in the following 24 months the Chrome browser would block third- party cookies. In April 2021, Google began releasing software updates to its Chrome browser with features intended to phase out third- party cookies. In May 2023, Google stated that it would deprecate third- party cookies by mid- 2024 **and in January 2024 started by deprecating third- party cookies for 1 % of users globally. In April 2024, Google announced that the deprecation of third- party cookies will not be completed in 2024** . Because we, and our ~~clients~~ **customers** , rely upon data, including that collected through cookies and similar technologies, it is possible that Google' s efforts may have a substantial impact on the ability to collect and use data from Internet users, and it is essential that we monitor developments in this area domestically and globally, and engage in responsible privacy practices, including providing consumers with notice of the types of data we collect and how we use that data to provide our services. In the U. S., the U. S. Congress and state legislatures, along with federal regulatory authorities have recently increased their attention on matters concerning the collection and use of consumer data. In the U. S., non- sensitive consumer data generally may be used under current rules and regulations, subject to certain restrictions, so long as the person does not affirmatively " opt- out " of the collection or use of such data. If an " opt- in " model were to be adopted in the U. S., less data would be available, and the cost of data would be higher. For example, California enacted legislation, the California Consumer Privacy Act (" CCPA "), that became operative on January 1, 2020 and came under California Attorney General (" AG") enforcement on July 1, 2020. The CCPA requires covered companies to, among other things, provide new disclosures to California consumers and afford such consumers new abilities to opt- out of certain sales of personal information, a concept that is defined broadly. The CCPA is the subject of regulations issued by the California AG. In November 2020 California voters also approved the ballot initiative known as the California Privacy Rights Act of 2020 (" CPRA "). Pursuant to the CPRA, effective January 1, 2023, the CCPA was amended by creating additional privacy rights for California consumers and additional obligations on businesses, which could subject us to additional compliance costs as well as possible fines, individual claims and commercial liabilities for certain compliance failures. Since the CCPA, ~~ten~~ **sixteen** other state legislatures so far have passed comprehensive privacy legislation, including Virginia, Colorado, Connecticut, Utah, Indiana, Iowa, Tennessee, Montana, Florida ~~and~~ **, Oregon,** Texas, **Delaware, Nebraska, New Hampshire, New Jersey and Kentucky** and other states have passed sector or data- specific legislation, such as Illinois ~~and~~ **,** Washington **, Nevada and Maryland** . Together with the CCPA and CPRA, these are referred to throughout as" State Consumer Privacy Acts." Each of these State Consumer Privacy Acts have gone, or will go, into effect on or before ~~July~~ **January** 1, ~~2025~~ **2026** . Many other states currently have comprehensive and / or sector or data- specific bills winding their way through their legislatures. In addition, the FTC Chair has..... costly expenditures to ensure continued compliance. We cannot yet predict the full impact of the State Consumer Privacy Acts on our business or operations, but they may require us to modify our data processing practices and policies and to incur substantial costs and expenses in an effort to comply. The State Consumer Privacy Acts have prompted a number of proposals for federal and other state privacy legislation that, if enacted, could increase our exposure to potential liability, add additional complexity to compliance in the U. S. market and increase our compliance costs. For example, other states have enacted or are considering legislation similar to that of the State Consumer Privacy Act statutory frameworks, including legislation that would require individuals to " opt- in " to the collection of certain consumer data. Decreased availability and increased costs of information could adversely affect our ability to meet our ~~clients~~ **customers** ' requirements and could result in decreased revenues ~~.~~ In addition,the FTC Chair has called for a new approach to consumer data protection,such as the notice and consent framework in which consumers are asked to agree to privacy policies.The FTC has also articulated and demonstrated its intention to use its authority under Section 5 of the Federal Trade Commission Act to focus on data privacy through investigations and enforcement actions (for unfair and deceptive actions),particularly in the areas of sensitive data,such as health,location,and children' s data,and has begun to demonstrate that with significant consent decrees.Further modifications and regulations under the State Consumer Privacy Acts,enforcement actions and guidance,or new rules promulgated by the FTC,could create additional liability and require costly expenditures to ensure continued compliance **.** . In Europe, the European General Data Protection Regulation (" GDPR") took effect on May 25, 2018 and applies to products and services that we provide in Europe, as well as the processing of personal data of EU citizens, wherever that processing occurs. The GDPR includes operational requirements for companies that receive or process personal data of residents of the European Union. For example, the GDPR requires offering a variety of controls to individuals in Europe before processing data for certain aspects of our service. In addition, the GDPR includes significant penalties for non- compliance of up to the greater of € 20 million or 4 % of an enterprise' s global annual revenue. Further, the European Union is expected to replace the EU Cookie Directive governing the use of technologies to collect consumer information with the ePrivacy Regulation. The replacement ePrivacy Regulation may impose burdensome requirements around obtaining consent and impose fines for violations that are materially higher than those imposed under the European Union' s current ePrivacy Directive and related EU member state legislation. In addition, some countries are considering or have passed legislation or interpretations implementing data protection requirements or requiring local storage and processing of data or similar requirements that could increase the cost and complexity of delivering our services. Any failure to achieve required data protection standards may result in lawsuits,

regulatory fines, or other actions or liability, all of which may harm our operating results. ~~In June 2016, a referendum was passed in the United Kingdom to leave the European Union, commonly referred to as " Brexit. " The United Kingdom exited the European Union pursuant to Brexit on January 31, 2020, subject to a transition period for certain matters that ran through December 31, 2020. Brexit has created an uncertain political and economic environment in the United Kingdom and other European Union countries. For example, a Data Protection Bill designed to be consistent with GDPR was enacted in the United Kingdom in May 2018, but it remains uncertain how data transfers to and from the United Kingdom will be regulated in the mid and long term. The full effect of Brexit is uncertain and depends on any agreements the United Kingdom may make to retain access to European Union markets. Consequently, no assurance can be given about the impact of the outcome and our business may be seriously harmed.~~ We are also subject to laws, regulations and other restrictions that dictate whether, how, and under what circumstances we can transfer, process and / or receive certain data that is critical to our operations, including data shared between countries or regions in which we operate, and data shared among our products and services. For example, in 2016, the European Union and the U. S. agreed to an alternative transfer framework for data transferred from the European Union to the U. S., called the Privacy Shield. On July 16, 2020, however, the European Court of Justice invalidated the Privacy Shield and companies may no longer rely on it as a valid mechanism to comply with European Union data protection requirements. ~~The invalidation of~~ **In July 2023,** the **EU adopted an adequacy decision for the EU- U. S. Data** Privacy ~~Shield and related uncertainty regarding~~ **Framework (" DPF"), allowing** ~~other~~ -- **the** ~~data~~ **DPF to facilitate the** transfer **of data from Europe to** ~~mechanisms could have a significant adverse impact on our operations, while increasing our compliance costs and legal and regulatory risks. While domestic efforts between~~ the ~~EU and~~ U. S. ~~toward a replacement are underway~~ , ~~the timing, requirements~~ and ~~reliability are unclear~~ **with the U. K. Extension, also from the U. K. to the U. S** . In addition, the other bases upon which we rely to legitimize the transfer of such data, such as Standard Contractual Clauses, have been subjected to regulatory and judicial scrutiny. If **any of** ~~other~~ -- **the** legal bases upon which we currently rely for transferring data from Europe to the U. S. are invalidated, if we are unable to transfer data between and among countries and regions in which we operate, or if we are prohibited from sharing data among our products and services, it could affect the manner in which we provide our services or adversely affect our financial results. In addition to government regulation, privacy advocacy and industry groups may propose new and different self- regulatory standards that either legally or contractually apply to us or our ~~clients~~ **customers** . We are members of self- regulatory bodies that impose additional requirements related to the collection, use, and disclosure of consumer data. Under the requirements of these self- regulatory bodies, in addition to other compliance obligations, we are obligated to provide consumers with notice about our use of cookies and other technologies to collect consumer data and of our collection and use of consumer data for certain purposes, and to provide consumers with certain choices relating to the use of consumer data. Some of these self- regulatory bodies have the ability to discipline members or participants, which could result in fines, penalties, and / or public censure (which could in turn cause reputational harm). Additionally, some of these self- regulatory bodies might refer violations of their requirements to the Federal Trade Commission or other regulatory bodies. Because the interpretation and application of privacy and data protection laws, regulations and standards are uncertain, it is possible that these laws, regulations and standards may be interpreted and applied in manners that are, or are asserted to be, inconsistent with our data management practices or the technological features of our solutions. If so, in addition to the possibility of fines, investigations, lawsuits and other claims and proceedings, it may be necessary or desirable for us to fundamentally change our business activities and practices or modify our products and services, which could have an adverse effect on our business. We may be unable to make such changes or modifications in a commercially reasonable manner or at all. Any inability to adequately address privacy concerns, even if unfounded, or any actual or perceived failure to comply with applicable privacy or data protection laws, regulations, standards or policies, could result in additional cost and liability to us, damage our reputation, decrease the availability of and increase costs for information, inhibit sales and harm our business. Furthermore, the costs of compliance with, and other burdens imposed by, the laws, regulations, standards and policies that are applicable to the businesses of our ~~clients~~ **customers** may limit the use and adoption of, and reduce the overall demand for, our platform. Privacy concerns, whether valid or not valid, may inhibit market adoption of our platform particularly in certain industries and foreign countries. Changes in tax laws or regulations that are applied adversely to us or our customers may have a material adverse effect on our business, cash flow, financial condition or results of operations. New income, sales, use or other tax laws, statutes, rules, regulations or ordinances could be enacted at any time, which could affect the tax treatment of our domestic and foreign earnings and materially affect our financial position and results of operations. For example, **in 2022** the United States ~~recently~~ passed the Inflation Reduction Act, which provides for a minimum tax equal to 15 % of the adjusted financial statement income of certain large corporations, as well as a 1 % excise tax on share repurchases, and the Organization for Economic Co- operation and Development issued proposals including the implementation of the global minimum tax under the Pillar Two model rule. Our existing corporate structure and intercompany arrangements have been implemented in a manner we believe is in compliance with current prevailing tax laws. However, due to economic and political conditions, tax rates and tax regimes in various jurisdictions may be subject to significant changes, and the tax benefits that we intend to eventually derive could be impacted by changing tax laws. Any new taxes could adversely affect our domestic and international business operations, and our business and financial performance. Further, existing tax laws, statutes, rules, regulations or ordinances could be interpreted, changed, modified or applied adversely to us, which could have a material adverse effect on our business, cash flow, financial condition or results of operations. Governments are increasingly focused on ways to increase tax revenue, which has contributed to an increase in audit activity, more aggressive positions taken by tax authorities and an increase in tax legislation. Any such additional taxes or other assessments may be in excess of our current tax provisions or may require us to modify our business practices in order to reduce our exposure to additional taxes going forward, any of which could have a material adverse effect on the Company' s business, results of operations and financial condition. Risks Related to Intellectual Property Third parties may claim that we are infringing their intellectual property and we could suffer significant litigation or

licensing expenses or be prevented from developing or selling products or services. Additionally, third parties may infringe our intellectual property and we may suffer competitive injury or expend significant resources enforcing our rights. As our business is focused on data- driven results and analytics, we rely heavily on proprietary information technology, processes and other protectable intellectual property rights. From time to time, third parties may claim that one or more of our products or services infringe their intellectual property rights. We analyze and take action in response to such claims on a case- by- case basis. Any dispute or litigation regarding patents or other intellectual property, whether they are with or without merit, could be costly and time- consuming due to the complexity of our technology and the uncertainty of intellectual property litigation, which could divert the attention of our management and key personnel away from our business operations, even if ultimately determined in our favor. A claim of intellectual property infringement could force us to enter into a costly or restrictive license or royalty agreement, which might not be available under acceptable terms or at all, could require us to pay significant damages (including attorneys' fees), could subject us to an injunction against development and sale of certain of our products or services, could require us to expend additional development resources to redesign our technology and could require us to indemnify our partners and other third parties. Our proprietary portfolio consists of various intellectual property rights, including patents, copyrights, database rights, source code, trademarks, trade secrets, know- how, confidentiality provisions and licensing arrangements. The extent to which such rights can be protected varies from jurisdiction to jurisdiction. If we do not enforce our intellectual property rights vigorously and successfully, our competitive position may suffer, which could harm our operating results. ~~32~~ **31**