Risk Factors Comparison 2024-08-07 to 2023-08-03 Form: 10-K

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

Our businesses routinely encounter and address risks, some of which may cause our future results to be different than we currently anticipate. The risk factors described below represent our current view of some of the most important risks facing our businesses and are important to understanding our business. The following information should be read in conjunction with Management' s Discussion and Analysis of Financial Condition and Results of Operations, Quantitative and Qualitative Disclosures About Market Risk and the consolidated financial statements and related notes included in this Annual Report on Form 10- K. This discussion includes a number of forward- looking statements. You should refer to the description of the qualifications and limitations on forward- looking statements in the first paragraph under Management' s Discussion and Analysis of Financial Condition and Results of Operations included in this Annual Report on Form 10- K. See" Item 1. Business — Competition" of this Form 10- K for a discussion of the competitive environment in the markets in which we operate. Many risks affect more than one category, and the risks are not in order of significance or probability of occurrence because they have been grouped by categories. The risks described below are not the only risks we face and the occurrence of any of the following risks or other risks not presently known to us or that we currently believe to be immaterial could have a materially adverse effect on our business, results of operations, financial condition or reputation. LEGAL AND COMPLIANCE RISKS Failure to comply with, compliance with or changes in, laws and regulations applicable to our businesses could have a materially adverse effect on our reputation, results of operations or financial condition, or have other adverse consequences Our business is subject to a wide range of complex U. S. and foreign laws and regulations, including, but not limited to, the laws and regulations described in the " Industry Regulation " section in Part I, Item 1 of this Annual Report on Form 10- K. Failure to comply with laws and regulations applicable to our operations or client solutions and services could cause us to incur substantial costs or could result in the suspension or revocation of licenses or registrations, the limitation, suspension or termination of services, the imposition of consent orders or civil and criminal penalties, including fines, and lawsuits, including class actions, that could damage our reputation and have a materially adverse effect on our results of operation or financial condition. In addition, changes in laws or regulations, or changes in the interpretation of laws or regulations by a regulatory authority, may decrease our revenues and earnings and may require us to change the manner in which we conduct some aspects of our business. For example, a change in regulations either decreasing the amount of taxes to be withheld or allowing less time to remit taxes to government authorities would adversely impact average client balances and, thereby, adversely impact interest income from investing client funds before such funds are remitted to the applicable ~~taxing~~ **tax** authorities. Changes in U. S. or foreign tax laws, regulations or rulings or the interpretation thereof could adversely affect our effective tax rate and our net income. Changes in laws, or interpretations thereof, that govern the co- employment arrangement between a professional employer organization and its worksite employees may require us to change the manner in which we conduct some aspects of our PEO business. In addition, changes in the manner in which health and welfare plans sponsored by PEOs or the TotalSource Health and Welfare Plan, in particular, are regulated could adversely impact the demand for our PEO offering. Because our PEO is a co- employer with our PEO clients and a Certified PEO by the Internal Revenue Service, we may be subject to certain obligations, responsibilities and liabilities of an employer with respect to Worksite Employees (WSE), including with respect to their wages and the payment thereof, the payment of certain taxes with respect to WSE wages and employee benefits provided to the WSEs. Even though PEO clients are contractually responsible for the timely remittance of such costs, it is possible that our clients will not remit such payments despite their contractual obligations. The risk of failing to receive such payments from PEO clients could be magnified during significant financial or other disruptions or catastrophic events, such as the failure of a bank ~~, like that of Signature Bank or Silicon Valley Bank,~~ with whom a significant number of PEO clients may bank at the time, or more widespread stress or failure within the U. S. banking system. Any such event could prevent or materially delay the recovery of any payments not timely remitted and could have an adverse impact on our financial results and liquidity. Our Wisely ® offerings and potentially other future offerings in the payments and / or consumer space may subject us to additional laws and regulations, some of which may not be uniform and may require us to modify or restrict our offerings and decrease our potential revenue and earnings. Failure to comply with anti- corruption laws and regulations, economic and trade sanctions, anti- money laundering laws and regulations, and similar laws could have a materially adverse effect on our reputation, results of operations or financial condition, or have other adverse consequences Regulators worldwide continue to exercise a high level of scrutiny with respect to anti- corruption, economic and trade sanctions, and anti- money laundering laws and regulations. Such scrutiny has resulted in aggressive investigations and enforcement of such laws and burdensome regulations, any of which could materially adversely impact our business. We operate our business around the world, including in numerous developing economies where companies and government officials are more likely to engage in business practices that are prohibited by domestic and foreign laws and regulations, including the United States Foreign Corrupt Practices Act and the U. K. Bribery Act 2010. Such laws generally prohibit improper payments or offers of payments to foreign government officials and leaders of political parties and, in some cases, to other persons, for the purpose of obtaining or retaining business. We are also subject to economic and trade sanctions programs, including those administered by the U. S. Treasury Department' s Office of Foreign Assets Control, which prohibit or restrict transactions or dealings with specified countries, their governments and, in certain circumstances, their nationals, and with individuals and entities that are specially designated, including narcotics traffickers and terrorists or terrorist organizations, among others. In addition, some of our businesses and entities in the U. S. and a number of other countries in which we operate are subject to anti- money laundering laws and regulations, including, for example, The Bank Secrecy Act of 1970, as amended

by the USA PATRIOT Act of 2001 (the " BSA "). Among other things, the BSA requires certain financial institutions, including banks and money services businesses (such as national trust banks and providers of prepaid access like us), to develop and implement risk- based anti- money laundering programs, report large cash transactions and suspicious activity, and maintain transaction records. We have registered our payroll card business as a provider of prepaid access, and registered ~~our~~ ADP Trust Bank **and ADP Retirement Trust Services** with the Treasury Department' s Financial Crimes Enforcement Network (FinCEN). **ADP Canada Co. is a registered entity with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) as a Money Service Business (MSB).** We have implemented policies and procedures to monitor and address compliance with applicable anti- corruption, economic and trade sanctions and anti- money laundering laws and regulations, and we regularly review, upgrade and enhance our policies and procedures. However, there can be no assurance that our employees, consultants or agents will not take actions in violation of our policies for which we may be ultimately responsible, or that our policies and procedures will be adequate or will be determined to be adequate by regulators. Any violations of applicable anti- corruption, economic and trade sanctions or anti- money laundering laws or regulations could limit certain of our business activities until they are satisfactorily remediated and could result in civil and criminal penalties, including fines, which could damage our reputation and have a materially adverse effect on our results of ~~operation~~ **operations** or financial condition. Further, bank regulators continue to impose additional and stricter requirements on banks to ensure they are meeting their BSA obligations, and banks are increasingly viewing money services businesses and third- party senders to be higher risk customers for money laundering. As a result, our banking partners that assist in processing our money movement transactions may limit the scope of services they provide to us or may impose additional material requirements on us. These regulatory restrictions on banks and changes to banks' internal risk- based policies and procedures may result in a decrease in the number of banks that may do business with us, may require us to materially change the manner in which we conduct some aspects of our business, may decrease our revenues and earnings and could have a materially adverse effect on our results of operations or financial condition. Failure to comply with privacy, data protection, artificial intelligence and cyber security laws and regulations could have a materially adverse effect on our reputation, results of operations or financial condition, or have other adverse consequencesThe collection, storage, hosting, transfer, processing, disclosure, use, security and retention and destruction of personal information required to provide our services is subject to federal, state and foreign privacy, data protection and cyber security laws. These laws, which are not uniform, generally do one or more of the following: regulate the collection, storage, hosting, transfer (including in some cases, the transfer outside the country of collection), processing, disclosure, use, security and retention and destruction of personal information; require notice to individuals of privacy practices; give individuals certain access and correction rights with respect to their personal information; and regulate the use or disclosure of personal information for secondary purposes such as marketing. Under certain circumstances, some of these laws require us to provide notification to affected individuals, clients, data protection authorities and / or other regulators in the event of a data breach. In many cases, these laws apply not only to third- party transactions, but also to transfers of information among the Company and its subsidiaries. The European Union (the " EU ") General Data Protection Regulation (the " GDPR "), and state consumer privacy laws like the California Privacy Rights Act of 2020 (the " CPRA "), are among the most comprehensive of these laws, and more and more jurisdictions are adopting similarly comprehensive laws that impose new data privacy protection requirements and restrictions. As part of our overall data protection compliance program in connection with the GDPR, we implemented Binding Corporate Rules (" BCRs ") as both a data processor and data controller, which permits us to process and transfer personal data across borders in compliance with EU data protection laws. We believe that providing insights and content from data, including via artificial intelligence (AI) and machine learning (ML), will become increasingly important to the value that our solutions and services deliver to our clients. We are increasingly leveraging AI and ML in our solutions and service delivery and are exploring how best to integrate generative AI technologies and develop and deploy capabilities that are beneficial to our clients and their employees. However, legislation that ~~would govern~~ **governs** the development and / or use of AI **has been adopted or** is under consideration in the U. S. at the state and local level, as well as abroad. In addition, self-regulatory frameworks like the National Institute of Standards and Technology AI Risk Management Framework are being promulgated and adherence to these may become an industry standard or a client expectation. As a result, the ability to provide data- driven insights and otherwise leverage AI and ML may be constrained by current or future laws **(including product liability regimes)** , regulatory or self- regulatory requirements or ethical considerations, including our own published, guiding ethical principles regarding AI and ML, that could restrict or impose burdensome and costly requirements on our ability to leverage data and / or these technologies in innovative ways. **Our use of generative AI in our products and operations also introduces additional risks, including risks related to accuracy, bias, security, and privacy. For example, if the data used to train a model or the model' s output is inaccurate or biased, or alleged to be inaccurate or biased, we could be subject to reputational damage or litigation.** Complying with privacy, data protection, AI and cyber security laws and requirements, including the enhanced obligations imposed by the GDPR, our BCRs ~~and~~ **, U. S. state privacy laws, including** the CPRA **, and the EU Artificial Intelligence Act** , may result in significant costs to our business and require us to amend certain of our business practices. Further, enforcement actions and investigations by regulatory authorities related to data security incidents and privacy violations continue to increase. The future enactment of more restrictive laws, rules or regulations and / or future enforcement actions or investigations could have a materially adverse impact on us through increased costs or restrictions on our businesses and noncompliance could result in significant regulatory penalties and legal liability and damage our reputation. In addition, data security events, concerns about privacy abuses by other companies and increased awareness of the potential (positive and negative) of AI are changing consumer and social expectations for enhanced protections (including with respect to bias and potential discrimination). As a result, noncompliance, the failure to meet such expectations or the perception of noncompliance or such failure, whether or not valid, may damage our reputation. If we fail to protect our intellectual property rights, it could materially adversely affect our business and our brandOur ability to compete and our success depend, in part,

upon our intellectual property. We rely on patent, copyright, trade secret and trademark laws, and confidentiality or license agreements with our employees, clients, vendors, partners and others to protect our intellectual property rights. We may need to devote significant resources, including cybersecurity resources, to monitoring our intellectual property rights. In addition, the steps we take to protect our intellectual property rights may be inadequate or ineffective, or may not provide us with a significant competitive advantage. Our intellectual property **(including source code)** could be wrongfully acquired as a result of a cyber-attack or other wrongful conduct by third parties or our personnel. Litigation brought to protect and enforce our intellectual property rights could be costly and time- consuming. Furthermore, our efforts to enforce our intellectual property rights may be met with defenses, counterclaims, and countersuits attacking the validity and enforceability of our intellectual property rights, which may be successful. In addition, use of AI tools may result in the release of confidential or proprietary information which could limit our ability to protect, or prevent us from protecting, our intellectual property rights. We may be sued by third parties for infringement of their proprietary rights, which could have a materially adverse effect on our business, financial condition or results of operationsThere is considerable intellectual property development activity in our industry. Third parties, including our competitors, may own or claim to own intellectual property relating to our products or services and may claim that we are infringing their intellectual property rights. Additionally, as we expand our use of AI, there is uncertainty regarding intellectual property ownership and license rights of AI algorithms and content generated by AI and we may become subject to similar claims of infringement. We may be found to be infringing upon third party intellectual property rights, even if we are unaware of their intellectual property rights. Any claims or litigation could cause us to incur significant expenses and, if successfully asserted against us or if we decide to settle, could require that we pay substantial damages or ongoing royalty payments, obtain licenses, modify applications, prevent us from offering our services, or require that we comply with other unfavorable terms. We may also be obligated to indemnify our clients, vendors or partners in connection with any such claim or litigation. Even if we were to prevail in such a dispute, any litigation could be costly and time- consuming. SECURITY AND TECHNOLOGY RISKSOur businesses collect, host, store, transfer, process, disclose, use, secure ~~and~~ **,** retain and dispose of personal and business information, and collect, hold and transmit client funds, and a security or privacy breach may damage or disrupt our businesses **or operations** , result in the disclosure of confidential information, damage our reputation, increase our costs, cause losses and materially adversely affect our results of operationsIn connection with our business, we collect, host, store, transfer, process, disclose, use, secure ~~and~~ **,** retain and dispose of large amounts of personal and business information about our clients, employees of our clients, our vendors and our employees, contractors and temporary staff, including payroll information, health care information, personal and business financial data, social security numbers and their foreign equivalents, bank account numbers, tax information and other ~~sensitive~~ personal and business information. We also collect significant amounts of funds from the accounts of our clients and transmit them to their employees, ~~taxing~~ **tax** authorities and other **payees** ~~third parties~~ . We are focused on ~~ensuring that we safeguard~~ **safeguarding** and ~~protect~~ **protecting** personal and business information and client funds, and we devote significant resources to maintain and regularly update our systems and processes. Nonetheless, the global environment continues to grow increasingly hostile as attacks on information technology systems continue to grow in frequency, complexity and sophistication **(including due to the use of AI)** , and we are regularly targeted by unauthorized parties using malicious tactics, code and viruses. Certain of these malicious parties may be state- sponsored and / or supported by significant financial and technological resources. Although this is a global problem, it may affect our businesses more than other businesses because malevolent parties (**which could** ~~including~~ **include** our personnel) may focus on the amount and type of personal and business information that our businesses collect, host, store, transfer, process, disclose, use, secure ~~and~~ **,** retain and dispose of, and the client funds that we collect and transmit. We have programs and processes in place **designed** to prevent, detect and respond to data or cybersecurity incidents. However, as a result of the complexity of our operating environment, the period over which hardware and software has been acquired or other reasons, our programs and processes may not be sufficient or adequate or may fail to prevent, detect or respond to a cybersecurity incident or identify and / or remediate a security vulnerability in our operating environment. The techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently, are increasingly more complex and sophisticated (including due to the use of AI). We may fail to anticipate or detect these techniques and / or incidents for long periods of time and, even when we do so, we may be unable or fail to implement adequate or timely preventive or responsive measures. Our ability to address data or cybersecurity incidents may also depend on the timing and nature of assistance that may be provided from relevant governmental or law enforcement agencies. Hardware, software, applications or services that we develop or procure from third parties, or are required by third parties such as foreign governments to install on our systems, may contain defects in design or manufacture or other problems that could (or, in respect of third- party software, may be designed to) compromise the confidentiality, integrity or availability of data or our systems. Unauthorized parties **have** also **attempted to gain (and in certain cases have gained), and will continue to** attempt to gain **,** access to our systems or facilities, or those of third parties with whom we do business, through fraud, trickery, or other methods of deceiving these third parties or our personnel, including phishing and other social engineering techniques whereby attackers use end- user behaviors to distribute computer viruses and malware into our systems or otherwise compromise the confidentiality, integrity or availability of data or our systems. As these threats continue to evolve and increase (including due to the use of AI), we continue to invest significant resources, and may be required to invest significant additional resources, to modify and enhance our ~~information security~~ **cybersecurity** ~~and~~ controls and to investigate and remediate any security vulnerabilities. In addition, while our operating environments are designed to safeguard and protect confidential personal and business information, we may not have the ability to monitor the implementation or effectiveness of any safeguards by our clients, vendors or partners and, in any event, third parties may be able to circumvent those security measures. Information **or system access** obtained by malevolent parties (**which could** ~~including~~ **include** our personnel) resulting from successful attacks against our clients, vendors, partners or other third parties may, in turn, be used to attack our information technology systems. **Further** ~~A cyberattack~~ , **while we perform due diligence prior to acquisitions and take actions to safeguard the businesses**

that we acquire, these businesses may not have invested as significantly as we do in security and technology and may be more susceptible to cybersecurity incidents, which may make us more vulnerable to cybersecurity incidents as well. We have been, and expect we will continue to be, the subject of cybersecurity attacks, including unauthorized intrusion, malicious software infiltration, network disruption, denial of service, corruption of data, ransomware attack, **and theft of sensitive information (including our intellectual property). Although none of the cybersecurity incidents that we have identified to date have materially affected us, including our business strategy, operations, results of operations, or financial condition, we continue to face significant known and unknown cybersecurity threats. In the future, a cybersecurity attack, unauthorized intrusion, malicious software infiltration, network disruption, denial of service, corruption of data, ransomware attack,** theft of non- public or other sensitive information, or similar act by a malevolent party (**which could** ~~including~~ **include** our personnel), or inadvertent acts or inactions by our vendors, partners or personnel, could result in the loss, disclosure or misuse of confidential personal or business information **or our intellectual property** or the theft of client or ADP funds, which could have a materially adverse effect on our business or results of operations or that of our clients, result in liability, litigation, regulatory investigations and sanctions or a loss of confidence in our ability to serve clients, or cause current or potential clients to choose another service provider. As the global environment continues to grow increasingly hostile, the security of our operating environment is ever more important to our clients and potential clients. As a result, the breach or perceived breach of our security systems could result in a loss of confidence by our clients or potential clients and cause them to choose another service provider, which could have a materially adverse effect on our business ~~. Although we believe that we maintain a robust program of information security and controls and none of the data or cybersecurity incidents that we have encountered to date have materially impacted us, a data or cyber security incident could have a materially adverse effect on our business, results of operations~~ , financial condition ~~and reputation~~ **or results of operations** . While ADP maintains insurance coverage that, subject to policy terms and conditions and a significant self- insured retention, is designed to address losses or claims that may arise in connection with certain aspects of data and cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in the continually evolving area of data and cyber risk. Our systems, applications, solutions and services may be subject to disruptions that could have a materially adverse effect on our business ~~and~~ **, operations, financial condition, results of operations or** reputationMany of our businesses are highly dependent on our ability to process, on a daily basis, a large number of complicated transactions. We rely heavily on our payroll, financial, accounting, and other data processing systems. We need to properly manage our systems, applications and solutions, and any upgrades, enhancements and expansions we may undertake from time to time, in order to ensure they properly support our businesses. From time to time, these systems, applications or solutions fail to operate properly or become disabled. Any such failure or disablement, even for a brief period of time, whether due to malevolent acts, errors, defects or any other factor (s), could result in financial loss, a disruption of our businesses **or operations** , liability to clients, loss of clients, regulatory intervention or damage to our reputation, any of which could have a materially adverse effect on our **business,** results of ~~operation~~ **operations** or financial condition. We have **a global business resiliency program that includes** disaster recovery, business continuity, and crisis management plans and procedures designed to protect our businesses against a multitude of events, including natural disasters, military or terrorist actions, power or communication failures, or similar events. Despite our preparations, our plans and procedures may not be successful in preventing or mitigating the loss of client data or funds, service interruptions, disruptions to our operations, or damage to our important facilities. In addition, the severity of the failure or disablement may require us to replace or rebuild the affected system (s), application (s) or solution (s) and we may be unable to do so before it materially adversely affects our business **or operations** . A disruption of the data centers or cloud-computing or other technology services or systems that we utilize could have a materially adverse effect on our ~~business~~We -- **business, operations, financial condition or results of operationsWe** host our applications and serve our clients with data centers that we operate, and with data centers that are operated, and cloud- computing and other technology services and systems that are provided, by third- party vendors. These data centers or cloud- computing and other technology services and systems have ~~(and, in the future, may)~~ failed, become disabled or been disrupted **, and may do so in the future** . Any failure, disablement or disruption, even for a limited period of time, could disrupt our businesses **or operations** and we could suffer financial loss, liability to clients, loss of clients, regulatory intervention or damage to our reputation, any of which could have a material adverse effect on our **business,** results of ~~operation~~ **operations** or financial condition. In addition, our third- party vendors may cease providing data center facilities or cloud- computing or other technology services or systems **(including those on which our products or services are based)** , elect to not renew their agreements **or licenses** with us on commercially reasonable terms or at all, breach their agreements **or licenses** with us or fail to satisfy our expectations, which could disrupt our operations and require us to incur costs which could materially adversely affect our results of ~~operation~~ **operations** or financial condition. BUSINESS AND INDUSTRY RISKSOur industry is subject to rapid technological change, including as a result of AI, and if we fail to upgrade, enhance and expand our technology and services to meet client needs and preferences, the demand for our solutions and services may materially diminishOur businesses operate in industries that are subject to rapid technological advances (such as AI) and changing client needs and preferences. In order to remain competitive and responsive to client demands, we continually upgrade, enhance, and expand our technology, solutions and services, including by leveraging AI in our solutions. If we fail to respond successfully to technology challenges and client needs and preferences or our competitors or other third parties respond to such challenges more quickly or successfully than us, the demand for our solutions and services may diminish. As new technologies (such as AI) continue to emerge, they may be disruptive to the HCM industry. These technologies could result in new and innovative HCM products and solutions that could increase competition, place us at a competitive disadvantage or even render obsolete our technology, products and solutions. In addition, investment in product development and new technologies often involves a long return on investment cycle. We have made and expect to continue to make significant investments in product development and new technologies. We must continue to dedicate a significant amount

of resources to our development efforts before knowing to what extent our investments will result in products the market will accept. In addition, our business could be adversely affected in periods surrounding our new product introductions if clients delay purchasing decisions to evaluate the new product offerings. Furthermore, we may not execute successfully on our product development strategy, including because of challenges with regard to product planning and timing and technical hurdles that we fail to overcome in a timely fashion. We may fail to realize all the economic benefit of our investment in the development of a product which could cause an impairment of goodwill or intangibles and result in a significant charge to earnings. We may not realize or sustain the expected benefits from our business transformation initiatives, and these efforts could have a materially adverse effect on our business, operations, financial condition, results of operations and competitive positionWe have been and will be undertaking certain transformation initiatives, which are designed to streamline our organization, extend our world- class distribution and strengthen our talent and culture, while supporting our revenue growth, margin improvement and productivity. If we do not successfully manage and execute these initiatives, or if they are inadequate or ineffective, we may fail to meet our financial goals and achieve anticipated benefits, improvements may be delayed, not sustained or not realized and our business, operations and competitive position could be adversely affected. These initiatives, or our failure to successfully manage them, could result in unintended consequences or unforeseen costs, including distraction of our management and employees, attrition, inability to attract or retain key personnel, and reduced employee productivity, which could adversely affect our business, financial condition, and results of operations. A major natural disaster or catastrophic event could have a materially adverse effect on our business, operations, financial condition and results of operations, or have other adverse consequencesOur business, operations, financial condition, results of operations, access to capital markets and borrowing costs may be adversely affected by a major natural disaster or catastrophic event, including civil unrest, geopolitical instability, war, terrorist attack, pandemics or other (actual or threatened) public health emergencies, extreme weather, such as droughts, hurricanes, flooding and wildfires (including as a result of climate change), or other events beyond our control, and measures taken in response thereto. The COVID- 19 outbreak created, and such other events may create, significant volatility and uncertainty and economic and financial market disruption. The extent of any such impact depends on developments which are highly uncertain and cannot be predicted, including the duration and scope of the event; the governmental and business actions taken in response thereto; actions taken by the Company in response thereto and the related costs; the impact on economic activity and employment levels; the effect on our clients, prospects, suppliers and partners; our ability to sell and provide our solutions and services, including due to travel restrictions, business and facility closures, and employee remote working arrangements; the ability of our clients or prospects to pay for our services and solutions; and how quickly and to what extent normal economic and operating conditions can resume. In addition, clients or prospects may delay decision making, demand pricing and other concessions, reduce the value or duration of their orders, delay planned work or seek to terminate existing agreements. Our business is also impacted by employment levels across our clients, as we have varied contracts throughout our business that blend base fees and per-employee fees. Political, economic and social factors may materially adversely affect our business and financial resultsTrade, monetary and fiscal policies, and political and economic conditions may substantially change, and credit markets may experience periods of constriction and volatility. A slowdown in the economy or other negative changes, including in employment levels, the level of interest rates or the level of inflation, may have a negative impact on our businesses. In addition, as our operating costs increase due to inflationary pressure or otherwise, we may not be able to offset these increases by corresponding price increases for our products and solutions. Clients may react to worsening conditions by reducing their spending on HCM services or renegotiating their contracts with us, which may adversely affect our business and financial results. We invest our funds held for clients in liquid, investment- grade marketable securities, money market securities, and other cash equivalents. Nevertheless, such investments are subject to general market, interest rate, credit and liquidity risks. These risks may be exacerbated, individually or together, during periods of unusual financial market volatility. In addition, as part of our client funds investment strategy, we extend the maturities of our investment portfolio for client funds and utilize short- term financing arrangements to satisfy our short- term funding requirements related to client funds obligations. In order to satisfy these short- term funding requirements, we maintain access to various sources of liquidity, including borrowings under our commercial paper program and our committed credit facilities, our ability to execute **regular** reverse repurchase transactions **, our committed reverse repurchase agreements,** and corporate cash balances. A reduction in the availability of any such financing during periods of disruption in the financial markets or otherwise may increase our borrowing costs and / or require us to sell available- for- sale securities in our funds held for clients to satisfy our short- term funding requirements. When there is a reduction in employment levels due to a slowdown in the economy, the Company may experience a decline in client fund obligations and may also sell available- for- sale securities in our funds held for clients in order to reduce the size of the funds held for clients to correspond to client fund obligations. A sale of such available- for- sale securities may result in the recognition of losses and reduce the interest income earned on funds held for clients, either or both of which may adversely impact our results of operations, financial condition and cash flow. In connection with our client funds assets investment strategy, we attempt to minimize the risk of not having funds collected from a client available at the time such client' s obligation becomes due by generally impounding the client' s funds at **or before** the time of payment of such client' s obligation. When we don' t impound client funds by the time we pay such client obligations (including for PEO clients with respect to which we are legally obligated for payroll and tax obligations in respect of WSEs as a Certified PEO), we are at risk of not recovering such funds or a material delay in such recovery. Such risk could be magnified during significant financial or other disruptions or catastrophic events, such as the failure of a bank with whom a significant number of clients may bank at the time or more widespread stress or failure within the U. S. banking system. Any such event could prevent or materially delay the recovery of any funds from clients and could have an adverse impact on our financial results and liquidity. We are dependent upon various large banks to execute electronic payments and wire transfers as part of our client payroll, tax and other money movement services. While we have contingency plans in place for bank failures, a systemic shutdown of the banking industry

would impede our ability to process funds on behalf of our payroll, tax and other money movement services clients and could have an adverse impact on our financial results and liquidity. We derive a significant portion of our revenues and operating income outside of the United States and, as a result, we are exposed to market risk from changes in foreign currency exchange rates that could impact our results of operations, financial position and cash flows. We publicly share certain information about our environmental, social and governance (" ESG ") initiatives, including our ~~net zero~~ **efforts related to** greenhouse gas emissions ~~pledge~~ **reductions and Inclusion, Diversity, Equity and Belonging efforts** . We may face increased scrutiny related to our ESG initiatives and any related targets, including from the investment community. In addition, our ability to achieve certain ESG initiatives and targets may depend on the actions or continuing requirements of governmental entities (e. g., our paperless initiatives may depend on whether certain states continue to require employers to offer employees **the option** to be paid ~~via~~ **by** paper check or to obtain employee consent to be paid electronically instead of ~~via~~ **by** paper check) **. There has also been an increase in current and proposed ESG regulations, standards and reporting requirements, which may result in legal and regulatory uncertainty as well as increased compliance costs for our business. Further, developments in the law relative to diversity may influence our talent strategies** . Our failure to achieve progress in these and other ESG areas on a timely basis, or at all, **our failure to fully comply with these new ESG requirements, or our failure to do so in a timely manner, or a negative perception of our ESG initiatives** could **adversely** impact our reputation, business, including employee **recruitment and** retention **, financial results** , and growth. Change in our credit ratings could adversely impact our operations and lower our profitabilityThe major credit rating agencies periodically evaluate our creditworthiness and have given us strong, investment- grade long- term debt ratings and high commercial paper ratings. Failure to maintain high credit ratings on long- term and short- term debt could increase our cost of borrowing, reduce our ability to obtain ~~intra~~ **short** - ~~day~~ **term** borrowing required by our ~~Employer Services~~ business, and adversely impact our results of operations. Our business could be negatively impacted as a result of actions by activist stockholders or othersWe **have been in the past, and** may be **in the future,** subject to actions or proposals from activist stockholders or others that may not align with our business strategies or the interests of our other stockholders. Responding to such actions could be costly and time- consuming, disrupt our business and operations, and divert the attention of our Board of Directors and senior management from the pursuit of our business strategies. Activist stockholders may create perceived uncertainties as to the future direction of our business or strategy, including with respect to our ESG efforts, which may be exploited by our competitors and may make it more difficult to attract and retain qualified personnel, potential clients and business partners and may affect our relationships with current clients, vendors, investors and other third parties. In addition, actions of activist stockholders may cause periods of fluctuation in our stock price based on temporary or speculative market perceptions or other factors that do not necessarily reflect the underlying fundamentals and prospects of our business. We may be unable to attract and retain qualified personnelOur ability to grow and provide our clients with competitive services is, to an important degree, dependent on our ability to attract and retain highly skilled and motivated people reflecting diverse perspectives and the diversity of our communities and clients. Competition for skilled employees in the outsourcing and other markets in which we operate is increasingly intense, making it more difficult and expensive to attract and retain highly skilled, motivated and diverse personnel. If we are unable to attract and retain highly skilled, motivated and diverse personnel, results of our operations and culture may suffer. In addition, the nature of the office environment and remote or hybrid working is changing, which may make it more difficult to attract and retain personnel. It may also present operational and workplace culture challenges that may adversely affect our business. 23