

Risk Factors Comparison 2025-02-10 to 2024-02-12 Form: 10-K

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

You should consider the risks described below in conjunction with the other information presented in this report. These risks have the potential to materially adversely affect the Company's business, results of operations or financial condition.

SUMMARY RISK FACTORS Some of the factors that could materially and adversely affect our business, financial condition, results of operations or prospects, include the following:

- Our results of operations and investments could be adversely affected by geopolitical or macroeconomic conditions;
- We are subject to significant uninsured exposures arising from errors and omissions, breach of fiduciary duty and other claims;
- We cannot guarantee that we are or will be in compliance with all current and potentially applicable U. S. federal and state or foreign laws and regulations, and actions by regulatory authorities or changes in legislation and regulation in the jurisdictions in which we operate could have a material adverse effect on our business;
- Our business or reputation could be harmed by our reliance on third- party providers or introducers;
- We may not be able to effectively identify and manage actual and apparent conflicts of interest;
- We could incur significant liability or our reputation could be damaged if our information systems are breached or we otherwise fail to protect client or Company data or information systems;
- The costs to comply with, or our failure to comply with, U. S. and foreign laws related to privacy, data security and data protection, such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act, as amended by the California Privacy Rights Act, (CCPA), **Australia's CPS 234, as well as emerging AI-related laws such as the EU's AI Act**, could adversely affect our financial condition, operating results and our reputation;
- Our business performance and growth plans could be negatively affected if we are not able to develop and implement improvements in technology or respond effectively to the threat of digital disruption and other technological change such as AI;
- The loss of members of our senior management team or other key colleagues, or if we are unsuccessful in our efforts to attract, retain and develop talent, could have a material adverse effect on our business;
- Failure to maintain our corporate culture ~~particularly in a hybrid work environment~~, **could damage adversely affect our business and** reputation;
- Increasing scrutiny and changing laws and expectations from regulators, investors, clients and our colleagues with respect to our environmental, social and governance (ESG) practices and disclosure may impose additional costs on us or expose us to new or additional risks;
- We face significant competitive pressures in each of our businesses, including from disintermediation, as our competitive landscape continues to evolve;
- We rely on a large number of vendors and other third parties to perform key functions of our business operations and to provide services to our clients. These vendors and third parties may act or fail to act in ways that could harm our business;
- Our inability to successfully recover should we experience a disaster or other business continuity or data recovery problem could cause material financial loss, loss of human capital, regulatory actions, reputational harm or legal liability;
- We face risks when we acquire or dispose of businesses;
- If we are unable to collect our receivables, our results of operations and cash flows could be adversely affected;
- We may not be able to obtain sufficient financing on favorable terms;
- Our defined benefit pension plan obligations could cause the Company's financial position, earnings and cash flows to fluctuate;
- Our significant non- U. S. operations expose us to exchange rate fluctuations and various risks that could impact our business;
- Our quarterly revenues and profitability may fluctuate significantly;
- Credit rating downgrades would increase our financing costs and could subject us to operational risk;
- Our current debt level could adversely affect our financial flexibility;
- The current U. S. tax regime has provisions which have unintended consequences and may also impact our tax rate in varying degrees based on where our global income is earned;
- We are exposed to multiple risks associated with the global nature of our operations;
- Results in our Risk and Insurance Services segment may be adversely affected by a general decline in economic activity;
- Volatility or declines in premiums and other market trends may significantly impede our ability to grow revenues and profitability;
- Adverse legal developments and future regulations concerning how intermediaries are compensated by insurers or clients, as well as allegations of anti- competitive behavior or conflicts of interest, could have a material adverse effect on Marsh's business, results of operations and financial condition;
- Mercer's Wealth business is subject to a number of risks, including risks related to public and private capital market fluctuations, third- party asset managers and custodians, operations and technology risks, **trading and execution risks**, conflicts of interest, ESG and greenwashing, asset performance and regulatory compliance, that, if realized, could result in significant damage to our business **; • Our businesses are subject to a number of risks related to the U. S. healthcare industry, including risks related to healthcare regulation and reputational damage from negative publicity**;
- Revenues for the services provided by our Consulting segment may decline for various reasons, including as a result of changes in economic conditions, the value of equity, debt and other asset classes, our clients' or an industry's financial condition or government regulation or an accelerated trend away from actively managed investments to passively managed investments;
- Factors affecting defined benefit pension plans and the services we provide relating to those plans could adversely affect Mercer; and
- The profitability of our Consulting segment may decline if we are unable to achieve or maintain adequate utilization and pricing rates for our consultants.

RISKS RELATING TO THE COMPANY GENERALLY

Macroeconomic Risks Our results of operations and investments could be adversely affected by geopolitical or macroeconomic conditions. Geopolitical and macroeconomic conditions, including from multiple major wars ~~escalating and global conflict~~ **conflicts** throughout the Middle East and rising tension in the South China Sea, slower GDP growth or recession, lower interest rates, capital markets volatility and, inflation **and changes in insurance premium rates** affect our clients' businesses and the markets they serve. These conditions, including inflationary expense pressure with our clients, may reduce demand for our services or depress pricing for those services, which could have a material adverse effect on our results of operations. For example, the war in Ukraine and the ~~escalating~~ conflict throughout the Middle East have resulted in worldwide geopolitical and

macroeconomic uncertainty and may negatively impact other regional and global economic markets (including Europe, the Middle East and the U. S.), companies in other countries (particularly those that have done business with Russia or have substantial exposure to, or operations in, impacted countries) and various sectors, industries and markets for securities and commodities globally, such as oil and natural gas, and may increase financial market volatility and adversely impact regional and global economic markets, industries and companies. ~~Moreover, the COVID-19 pandemic impacted businesses, including our clients, third-party vendors and business partners, globally in every geography in which we operate. In addition, the potentially divergent laws and regulations as a result of Brexit may continue to lead to economic and legal uncertainty, causing increased economic volatility or disrupting the markets and clients we serve.~~ Changes in macroeconomic and geopolitical conditions could also shift demand to services for which we do not have a competitive advantage, and this could negatively affect the amount of business that we are able to obtain. More generally, our investments, including our minority investments in other companies as well as our cash investments and those held in a fiduciary capacity, are subject to general credit, liquidity, counterparty, foreign exchange, market and interest rate risks. For example, fluctuations in interest rates and foreign exchange rates between the U. S. dollar and foreign currencies may adversely affect our results of operations. Lower interest rates may lead to a decline in our fiduciary income. These risks may be exacerbated by global macroeconomic conditions, market volatility and regulatory, financial and other difficulties affecting the companies in which we have invested or that may be faced by financial institution counterparties. During times of stress in the banking industry, counterparty risk can quickly escalate, potentially resulting in substantial trading and investment losses for corporate and other investors. In addition, we may incur investment losses as a result of unusual and unpredictable market developments, and we may experience lower earnings if the yields on investments begin to decline. If the banking system or the fixed income, interest rate, credit or equity markets deteriorate, the value and liquidity of our investments could be adversely affected. Finally, the value of the Company's assets held in other jurisdictions, including cash holdings, may decline due to foreign exchange fluctuations. Legal and Regulatory Risks We are subject to significant uninsured exposures arising from errors and omissions, breach of fiduciary duty and other claims. Our businesses provide numerous professional services, including the placement of insurance and the provision of consulting, investment advisory, investment management and actuarial services, to clients around the world. As a result, the Company and its subsidiaries are subject to a significant number of errors and omissions, breach of fiduciary duty, breach of contract and similar claims, which we refer to collectively as "E & O claims." In our Risk and Insurance Services segment, such claims include allegations of damages arising from our failure to assess clients' risks, advise clients, place coverage, or notify insurers of potential claims on behalf of clients in accordance with our obligations to them. For example, these claims could include allegations related to losses from cyberattacks associated with policies where cyber risk was not specifically included or excluded in policies, commonly referred to as "silent cyber." In our Consulting segment, where we increasingly may act in a fiduciary capacity through our investments business, such claims could include allegations of damages arising from the provision of consulting, investment management (including, for example, from trading execution or other operational errors), actuarial, pension administration and other services. We may also be exposed to claims related to services or solutions offered by the Consulting segment in addition to consulting services. These Consulting segment services frequently involve complex calculations and services, including (i) making assumptions about, and preparing estimates concerning, contingent future events, (ii) drafting and interpreting complex documentation governing pension plans, (iii) calculating benefits within complex pension structures, (iv) providing individual financial planning advice including investment advice and advice relating to cashing out of defined benefit pension plans, (v) providing investment advice, including guidance on asset allocation and investment strategy, and (vi) managing client assets, including the selection of investment managers and implementation of the a client's investment policy and strategies. We provide these services to a broad client base, including clients in the public sector. Matters may relate to services provided by the Company dating back many years. Such claims may subject us to significant liability for monetary damages, including punitive and treble damages, negative publicity and reputational harm, and may divert personnel and management resources. We may be unable to effectively limit our potential liability in certain jurisdictions, including through insurance, or in connection with certain types of claims, particularly those concerning claims of a breach of fiduciary duty. In establishing liabilities for E & O claims in accordance with U. S. generally accepted accounting principles ("U. S. GAAP"), the Company uses case level reviews by inside and outside counsel, actuarial analysis by Oliver Wyman, a subsidiary of the Company, and other methods to estimate potential losses. A liability is established when a loss is both probable and reasonably estimable. The liability is assessed quarterly and adjusted as developments warrant. In many cases, the Company has not recorded a liability, other than for legal fees to defend a claim, because we are unable, at the present time, to make a determination that a loss is both probable and reasonably estimable. Given the judgment involved in estimating and establishing such liabilities, as well as the unpredictability of E & O claims and the litigation that can flow from them, it is possible that an adverse outcome in a particular matter could have a material adverse effect on the Company's business, results of operations or financial condition. We cannot guarantee that we are or will be in compliance with all current and potentially applicable U. S. federal and state or foreign laws and regulations, and actions by regulatory authorities or changes in legislation and regulation in the jurisdictions in which we operate could have a material adverse effect on our business. Our activities are subject to extensive regulation under the laws of the U. S. and its various states, the United Kingdom, the European Union and its member states, Australia and the other jurisdictions in which we operate. We are also subject to trade sanctions laws relating to countries such as Afghanistan, Belarus, Cuba, Iran, North Korea, Russia, Syria, Ukraine (Russia-controlled territories) and Venezuela, and anti-corruption laws such as the U. S. Foreign Corrupt Practices Act and the U. K. Bribery Act. We are subject to numerous other laws on matters as diverse as internal control over financial reporting and disclosure controls and procedures, securities regulation, data privacy and protection, cybersecurity, taxation, anti-trust and competition, immigration, wage- and- hour standards and employment and labor relations. The U. S. and foreign laws and regulations that apply to our operations are complex and may change rapidly, and our efforts to comply and keep up with them require significant resources. In some cases,

these laws and regulations may decrease the need for our services, increase our costs, negatively impact our revenues or impose operational limitations on our business, including on the products and services we may offer or on the amount or type of compensation we may collect. In **addition-particular**, the financial and operational impact of complying with laws and regulations has increased in the current **global** environment of increased regulatory activity and enforcement. **In addition, in the United States, shifts in regulatory priorities, policy approaches or interpretations of existing laws by federal, state or local governments occur following changes in U. S. presidential administrations, which often leads to changes involving the level of regulatory oversight and focus on businesses and certain industries, particularly financial services.** Changes **or uncertainty** with respect to the applicable laws and regulations may impose additional and unforeseen costs on us or pose new or previously immaterial risks to us. There can be no assurance that current and future government regulations will not adversely affect our business, and we cannot predict new regulatory priorities, the form, content or timing of regulatory actions, and their impact on our business and operations. In addition, geopolitical conflict, such as the war in Ukraine and the **escalating** conflict throughout the Middle East, has resulted in, and may continue to result in, new and rapidly evolving trade sanctions, which may increase our costs, negatively impact our revenues or impose additional operational limitations on our businesses. **Changes to tax laws, trade agreements, tariffs, labor policies, or environmental standards could also result in increased costs or operational changes.** While we attempt to comply with applicable laws and regulations, there can be no assurance that we, our **employees-colleagues**, our consultants and our contractors and other agents are in full compliance with such laws and regulations or interpretations at all times, or that we will be able to comply with any future laws or regulations. If we fail to comply or are accused of failing to comply with applicable laws and regulations, including those referred to above, or new and evolving regulations regarding cybersecurity, AI or **sustainability** ~~environmental, social and governance~~ matters, we may become subject to investigations, criminal penalties, civil remedies or other consequences, including fines, injunctions, loss of an operating license or approval, increased scrutiny or oversight by regulatory authorities, the suspension of individual employees, limitations on engaging in a particular business or redress to clients or other parties, and we may become exposed to negative publicity or reputational damage. Moreover, our failure to comply with laws or regulations in one jurisdiction may result in increased regulatory scrutiny by other regulatory agencies in that jurisdiction or regulatory agencies in other jurisdictions. These inquiries consume significant management attention, and the cost of compliance and the consequences of failing to be in compliance could therefore have a material adverse effect on our business. In most jurisdictions, government regulatory authorities have the power to interpret and amend or repeal applicable laws and regulations, and have discretion to grant, renew and revoke the various licenses and approvals we need to conduct our activities. Such authorities may require the Company to incur substantial costs in order to comply with such laws and regulations. In some areas of our businesses, we act on the basis of our own or the industry's interpretations of applicable laws or regulations, which may conflict from state to state or country to country. In the event those interpretations eventually prove different from the interpretations of regulatory authorities, we may be penalized or precluded from carrying on our previous activities. Moreover, the laws and regulations to which we are subject may conflict among the various jurisdictions and countries in which we operate, which increases the likelihood of our businesses being non-compliant in one or more jurisdictions. In addition, we may be responsible for the legal and regulatory liabilities of companies that we acquire. Additional information regarding certain ongoing investigations and certain other legal and regulatory proceedings is set forth in Note 16, Claims, Lawsuits and Other Contingencies, in the notes to the consolidated financial statements included under Part II, Item 8 of this report. Our business or reputation could be harmed by our reliance on third-party providers or introducers. We currently utilize the services of hundreds of third-party providers to meet the needs of our clients around the world. There is a risk that our third-party providers or introducers engage in business practices that are prohibited by our internal policies or violate applicable laws and regulations, such as the U. S. Foreign Corrupt Practices Act and the U. K. Anti-Bribery Act. We may not be able to effectively identify and manage actual and apparent conflicts of interest. Given the significant volume of our engagements, potential conflicts of interest may arise across our businesses. There is a risk that we may not effectively identify and manage potential conflicts of interest, including but not limited to where our services to a client conflict, or are perceived to conflict, with the interests of another client or our own interests, where we receive revenue or benefits from third-parties with whom we conduct business (including but not limited to insurers, investment managers and vendors) and where our colleagues have personal interests. **Cybersecurity, Data Protection and Technology Risks** We could incur significant liability or our reputation could be damaged if our information systems are breached or we otherwise fail to protect client or Company data or information systems. In operating our business and providing services and solutions to clients, we collect, use, store, transmit and otherwise process certain electronic information, including personal, confidential, proprietary and sensitive data such as financial records, health care, mergers and acquisitions and personal data of our clients, colleagues and vendors. We rely on the efficient, uninterrupted and secure operation of complex information technology systems and networks to operate our business and securely process, transmit and store electronic information. In the normal course of business, we also share electronic information with our vendors and other third parties, **which in some cases is critical to our ability to deliver services to our clients.** This electronic information comprises sensitive and confidential data, including information related to financial records, health care, mergers and acquisitions and clients' personal data. Our information technology systems and information security control systems, and those of our numerous third-party providers, as well as the control systems of critical infrastructure they rely on, such as power grids, and undersea cables, are potentially vulnerable to unauthorized access, damage or interruption from a variety of external threats, including software bugs, physical attack, cyberattacks, computer viruses and other malware, malicious or destructive code, ransomware, social engineering attacks (including **phishing-phishing, business e-mail compromise** and digital or telephonic impersonation), hacking **theft**, denial-of-service attacks and other types of data and systems-related modes of attack. The techniques used to achieve such unauthorized access, damage or interruption change frequently and new techniques may not be identified until they are launched against a target, and we may be unable to anticipate these techniques or implement adequate preventative or

remedial measures, resulting in potential data loss, data unavailability, data corruption or other damage to information technology systems. In addition, remote and hybrid work arrangements have increased the risk of phishing and other cybersecurity attacks, unauthorized dissemination of personal, confidential, proprietary or sensitive data, and unauthorized access to company computing assets. Further, a disruption of physical infrastructure could impact our ability to conduct business and service clients. This may include deliberate or unintentional disruption of service to electrical systems, satellite communications, undersea or terrestrial cable systems, Internet services, or other systems our colleagues or third parties rely on us to conduct business in a multitude of jurisdictions across the globe. Disruptions may be the result of weather, natural disaster, war, terrorism, pandemic, or other natural or geopolitical events. Our systems are also subject to compromise from internal threats such as fraud, ~~mistake~~ **mistakes**, misconduct or other improper action by employees, vendors and other third parties with otherwise legitimate access to our systems. Moreover, we face the ongoing challenge of managing access controls in a complex environment. The latency of a compromise is often measured in months but could be years, and we may not be able to detect a compromise in a timely manner, and even if detected, there can be no assurance that we can mitigate or remediate such compromise in an adequate or timely manner. We could experience significant financial and reputational harm if our information systems are breached, sensitive client or Company data are compromised, surreptitiously modified, rendered inaccessible for any period of time or maliciously made public, or if we fail to make adequate or timely disclosures to the public, law enforcement agencies or regulators following any such event, whether due to delayed discovery or a failure to follow existing protocols. Cyberattacks are increasing in frequency and evolving in nature. We are at risk of attack by a variety of adversaries, including nation states, state-sponsored organizations, **opportunistic attacks, and** organized crime and hackers, through use of increasingly sophisticated methods of attack, including the deployment of AI to find and exploit vulnerabilities," deep fakes", long-term, persistent attacks (referred to as advanced persistent threats) and the use of the IT supply chain to introduce malware through software updates or compromised suppliers accounts or hardware. In particular, the advance of AI and large language models has given rise to additional vulnerabilities and potential entry points for cyber threats. With generative AI tools, threat actors may have additional tools to automate breaches or persistent attacks, evade detection, or generate sophisticated phishing emails or other forms of digital impersonation, **doing so quickly and without requiring deep technical understanding of potential exploits**. In addition, increasing use of generative AI models in our internal systems may create new attack methods for adversaries. Because generative AI is a new field, understanding of cybersecurity risks and protection methods continues to develop, and features that rely on generative AI, including in services provided to us by third parties, may be susceptible to unanticipated cybersecurity threats from sophisticated adversaries and other cybersecurity incidents. Further, we are at increased risk of a cyberattack during periods of heightened geopolitical conflict, such as the war in Ukraine and the ~~escalating~~ conflict throughout the Middle East, as diplomatic events and economic policies may trigger espionage or retaliatory cyber incidents. **Additionally, nation states may deploy threat actors masquerading as potential candidates for hire at target companies to perform corporate espionage or execute internal cyber threat activities**. Despite our efforts to comply with applicable cybersecurity requirements and mitigate risks of cybersecurity threats, we cannot be certain that our security measures will definitively prevent, contain, detect, or remediate all cybersecurity threats or incidents or other instructions from malware currently in existence or developed in the future. As the breadth and complexity of the technologies we use and the software and platforms we develop continue to grow, including as a result of the use of mobile devices, cloud services, "open source" software, social media tools and the increased reliance on devices connected to the Internet (known as the "Internet of Things"), the potential risk of security breaches and cyber-attacks also increases. Despite ongoing efforts to improve our ability to protect data from compromise, we may not be able to protect all of our data across our diverse systems. Our efforts to improve and protect data from compromise may also identify previously undiscovered instances of security breaches or other cyber incidents. Our policies, employee training (including phishing prevention training), procedures and technical safeguards may also be insufficient to prevent, detect or remediate improper access to confidential, personal or proprietary information. In addition, the competition for talent in the data privacy and cybersecurity space is intense, and we may also be unable to hire, develop or retain suitable talent capable of adequately detecting, mitigating or remediating these risks. Should an attacker gain access to our network using compromised credentials of an authorized user, we are at risk that the attacker might successfully leverage that access to compromise additional systems and data. Certain measures that could increase the security of our systems, such as data encryption (including encryption of data at rest), heightened monitoring and logging, scanning for source code errors or deployment of multi-factor authentication, take significant time and resources to deploy broadly, and such measures may not be deployed in a timely manner or be effective against an attack. The inability to implement, maintain and upgrade adequate safeguards could have a material adverse effect on our business. Our information systems must be continually updated, patched, and upgraded to protect against known vulnerabilities. The volume of new software **and infrastructure** vulnerabilities ~~has continues to increased~~ **increase** markedly, as has the criticality of patches and other mitigation and remedial measures. In addition to mitigating and remediating newly identified vulnerabilities, previously identified vulnerabilities must also be continuously addressed. Accordingly, we are at risk that cyberattackers exploit these ~~known~~ vulnerabilities before they have been communicated by vendors or addressed. Due to the large number and age of the systems and platforms that we operate, the increased frequency at which vendors are issuing security patches to their products, the need to test patches and, in some cases, **coordinate with clients and vendors, before they can be deployed, we perpetually face the substantial risk that we cannot deploy patches in a timely manner**. **Some security patches may not be compatible with other software running on our systems and therefore may not be able to be deployed**. We are also dependent on third party vendors to keep their systems patched and secure in order to protect our data. Any failure related to these activities could have a material adverse effect on our business. We have numerous vendors and other third parties who receive personal information from us in connection with the services we offer our clients and our employees. We also use hundreds of IT vendors and software providers to maintain and secure our global information systems infrastructure. In addition, we have migrated

certain data, and may increasingly migrate data, to the cloud where it is hosted by third-party providers. Some of these vendors and third parties also have direct access to our systems or data. We are at risk of a cyberattack involving a vendor or other third party parties, which could result in a breakdown of such third party's data protection processes or the cyberattackers gaining access to our infrastructure or data through a supply chain attack. Highly publicized data security breaches, such as the October 2023 attack on Okta, may embolden malicious actors to target the IT supply chain and providers of business software. **In addition, we depend on our third-party vendors to keep software current. Our systems' availability could be impacted by poor or improperly tested software code and updates deployed to our environment by a third-party through normal and expected processes, which occurred with the CrowdStrike event in July 2024.** Our control over and ability to monitor the cybersecurity practices of our third-party vendors and service providers, and other third parties with whom we do business, remains limited, and there can be no assurance that we can prevent, mitigate, or remediate the risk of any compromise or failure in the **development processes or** cybersecurity infrastructure **or IT controls** owned or controlled by such third parties. Additionally, any contractual protections with such third parties, including our right to indemnification, if any, may be limited or insufficient to prevent a negative impact on our business from such compromise or failure. We have a history of making acquisitions and investments. The process of integrating the information systems of any businesses we acquire is complex and exposes us to additional risk. For instance, we may not adequately identify weaknesses and vulnerabilities in an acquired entity's information systems, either before or after the acquisition, which could affect the value we are able to derive from the acquisition, expose us to unexpected liabilities or make our own systems more vulnerable to a cyberattack. In addition, if we discover a historical compromise, security breach or other cyber incident related to the target's information systems following the close of the acquisition, we may be liable and exposed to significant costs and other unforeseen liabilities. We may also be unable to integrate the systems of the businesses we acquire into our environment in a timely manner, which could further increase these risks until such integration takes place. We have experienced data incidents and cybersecurity breaches, such as malware incursions (including computer viruses and ransomware), vulnerabilities in the software on which we rely, users exceeding their data access authorization, employee misconduct and incidents resulting from human error, such as emails sent to the wrong recipient, loss of portable and other data storage devices or misconfiguration of software or hardware resulting in inadvertent exposure of personal, sensitive, confidential or proprietary information. ~~In April 2021, an unauthorized actor leveraged a vulnerability in a third-party's software and gained access to a limited set of data in our~~ **or environment reduction of system availability.** Like many companies, we are also subject to social engineering attacks such as WhatsApp scams and regular phishing email campaigns directed at our employees that can result in malware infections, fraud and data loss. Although these incidents have resulted in data loss and other damages, to date, they have not had a material adverse effect on our business or operations. In the future, these types of incidents could result in personal, sensitive, confidential or proprietary information, including client, employee or Company data, being lost or stolen, surreptitiously modified, rendered inaccessible for any period of time, or maliciously made public, which could have a material adverse effect on our business. In the event of a cyberattack, we might have to take our systems offline, which could interfere with services to our clients or damage our reputation. A cyberattack may also result in systems or data being encrypted or otherwise unavailable due to ransomware or other malware. We also may be unable to detect an incident, assess its severity or impact, or appropriately respond in a timely or adequate manner. In addition, our liability insurance, which includes cyber insurance, may not be sufficient in type or amount to cover us against claims related to security breaches, cyberattacks and other related data and system incidents. Further, we cannot be sure that our existing coverage will continue to be available on acceptable terms or at all or that our insurers will not deny coverage as to any future claim. The costs to comply with, or our failure to comply with, U. S. and foreign laws related to privacy, data security and data protection, such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act, as amended by the California Privacy Rights Act, (CCPA), **Australia's CPS 234, as well as emerging AI-related laws such as the EU's AI Act,** could adversely affect our financial condition, operating results and our reputation. Improper collection, use, disclosure, cross border transfer, retention and other processing of confidential, personal, or proprietary data could result in regulatory scrutiny, legal and financial liability, or harm to our reputation. In operating our business and providing services and solutions to clients, we store and transfer sensitive employee and client data, including personal data, in and across multiple jurisdictions. We collect data from ~~client~~ **clients** and individuals located all over the world and leverage systems and teams to process it. As a result, we are subject to a variety of laws and regulations in the U. S., Europe and around the world regarding privacy, data protection, data security and cyber security. These laws and regulations are continuously evolving and developing. Some of these laws and regulations are increasing the level of data handling restrictions, including rules on data localization, all of which could affect our operations and result in regulatory liability and high fines. In particular, high-profile data breaches at major companies continue to be disclosed regularly, which is leading to even greater regulatory scrutiny and **significant fines, which at the highest levels they have ever been.** These fines are not limited to data breaches ~~and as regulators are increasingly focusing~~ **focus** on other data processing activities, including those related to ad-tech and "data subject" rights. The number of laws that apply to us keeps increasing and the interpretation of such laws is often uncertain and may be conflicting. At the international level, we are subject to an increasing number of comprehensive privacy laws including, for example, those passed in Indonesia, the Kingdom of Saudi Arabia ~~and~~, **India and Australia**. Many of these laws, which are modeled after the GDPR, have greatly increased the jurisdictional reach of privacy laws and added a broad array of requirements for handling personal data, such as the public disclosure of data breaches, data protection impact assessments, data portability and the appointment of data protection officers in some cases. ~~Following the UK's withdrawal from the EU, we are also subject to the UK General Data Protection Regulation ("UK GDPR"), a version of the GDPR as implemented into UK law, and this law may not mirror the GDPR, thereby adding operational complexity and legal risk.~~ Given the breadth and depth of changes in data protection obligations, including classifying data and committing to a range of administrative, technical and physical controls to protect data and enable data transfers across borders, our compliance with such laws will continue to

require time, resources and review of the technology and systems we use. Despite a proliferation of regulatory guidance papers, there remains uncertainty in key areas related to these laws, and that uncertainty could result in potential liability for our failure to meet our obligations, including the possibility of significant fines some of which can amount to 4 % or more of our global revenue. Further, despite recent developments such as the U. S.- EU Data Privacy Framework and the U. S.-UK-U. K. Data Bridge, there remains a high level of uncertainty concerning the future of the flow of personal information between the U. S. and EU, between the U. S. and the UK-U. K. and between the UK-U. K. and the EU. This, and that uncertainty may impair our ability to offer our existing and planned products and services or increase our cost of doing business. Some of the global laws enacted in recent years, including those in China and the Kingdom of Saudi Arabia, also include data localization elements that will require that certain personal data stay within their borders. These requirements are complex and our efforts to comply with them require significant resources, and we cannot guarantee we are or will be in full compliance with such laws at all times. At the U. S. federal level, we are subject to various privacy laws and regulations, including those promulgated under the authority of the U. S. Federal Trade Commission, which has the authority to regulate and enforce against unfair or deceptive acts or practices in or affecting commerce, including with respect to data privacy and cybersecurity. At the U. S. state level, we are subject to laws and regulations related to privacy, such as the CCPA, which introduced concepts such as transparency and rights like access and deletion, that have been enacted by over twenty a dozen states with many more on the verge of enacting such laws expected to pass in future years. These laws establish a privacy framework for covered businesses, including various obligations imposed on them related to the personal information they collect and use, and offer various rights for their state residents. Some of these laws provide a private right of action for violations and in some cases damages may be significant. Many of these laws diverge from the CCPA and create their own set of rules, and this proliferation of inconsistent state level privacy laws will add operational complexity and increased risk of noncompliance or violations which could trigger enforcement action or litigation. In addition to data protection and data privacy laws, foreign countries and U. S. states are enacting AI and cybersecurity laws and regulations. For example, in late 2023 the New York State Department of Financial Services (NYDFS) issued amendments to its previous cybersecurity regulations which imposed obligations on companies such as Marsh McLennan, including for example, requiring companies to provide evidence of how they are implementing their data retention, data governance and data classifications policies and procedures. A number of states have also adopted laws covering data collected by insurance licensees that include security and breach notification requirements. All of these evolving compliance and operational requirements impose significant costs that are likely to increase over time, may divert resources from other initiatives and projects and could restrict the way services involving data are offered, all of which may adversely affect our results of operations. **Failure to comply with some of these obligations, especially those related to data retention requirements, could expose us to regulatory fines and other penalties.** Many statutory requirements, both in the U. S. and abroad, include obligations for companies to notify individuals of security breaches involving certain personal information, which could result from breaches experienced by us or our vendors. For example, laws in all 50 U. S. states generally require businesses to provide notice under certain circumstances to consumers whose personal information has been disclosed as a result of a breach. In addition to government regulation, our agreements with certain third parties may require us to notify them in the event of a security breach. Further, privacy advocates and industry groups have and may in the future propose self-regulatory standards. These laws, rules and industry standards may legally or contractually apply to us, or we may elect to comply with them. We expect that there will continue to be new proposed laws and regulations concerning data privacy and security, and we cannot yet determine the impact such future laws, regulations and standards may have on our business. Many of these laws and rules also include strict notification requirements for organizations related to confirmed or suspected breaches. This narrow notification window is often too short to fully validate the facts, and there is an increased risk of reporting a false alarm or immaterial breach, which may lead to reputational damage despite there not being an actual data breach. We post public privacy policies notices and other documentation regarding our collection, use, disclosure, cross-border transfer, retention, and other processing of personal information. Although we endeavor to comply with our published policies notices and other documentation, we may at times fail to do so or may be perceived to have failed to do so. Moreover, despite our efforts, we may not be successful in achieving compliance if our employees, contractors, service providers, vendors or other third parties with whom we do business fail to comply with our published policies notices and documentation. Such failures could carry similar consequences or subject us to potential enforcement actions or investigations if they are found to be deceptive, unfair or misrepresentative of our actual practices. Furthermore, **U. S. and global regulators continue to focus their enforcement actions and investigations by regulatory authorities on website-related practices to data security incidents and privacy violations, including the proper use of an ongoing focus on compliance related to website "cookies", pixels and other online trackers, as well as the use of online session recording tools. As we use such tools in some countries or our website environment, we are at risk of being impacted by such activity, including fines and cease and desist orders. Additionally, certain foreign, U. S. federal and U. S. states- state governments are increasingly enacting, or are considering enacting, AI-related laws and regulations, such as the EU's AI Act, the AI Transparency Act of California and the AI Act of Colorado, which impose complex new obligations on developers and providers of AI systems. Given the emerging nature of AI technology, the lack of legal or regulatory precedent, and the ambiguity surrounding key definitions, complying with these evolving legal and regulatory frameworks is likely to be both challenging and costly. There is a risk that we may not fully meet the requirements set forth by these laws and regulations, potentially exposing us to legal, regulatory or financial penalties. Furthermore, as new and divergent AI laws and regulations continue to emerge globally, they could significantly increase our risk of liability and fines, impact our ability to deploy and utilize AI tools across different jurisdictions, disrupt operations and prospective business and increase our compliance burdens.** Privacy or AI-related legal or regulatory violations, including unauthorized use disclosure or transfer of sensitive, personal or confidential client or Company data, whether through systems failure, employee negligence, fraud or misappropriation, by the Company, our vendors

or other parties with whom we do business (if they fail to meet the standards we impose) could damage our reputation and subject us to significant litigation, monetary damages, regulatory enforcement actions, fines and criminal prosecution in one or more jurisdictions **where we operate**. Given the complexity of operationalizing the various privacy, **data security, data protection and AI laws and regulations** mentioned above, the **complexity maturity level** of proposed compliance frameworks and the continued lack of certainty on how to implement their requirements, we and our clients are at risk of enforcement actions taken by **data protection-applicable regulators or** authorities around the world or litigation from **third parties, including** consumer advocacy groups acting on behalf of data subjects. ~~We~~ **Additionally, due to the ongoing fast pace of legislative and regulatory activity, we** may not be able to respond quickly or effectively to **new legislative, regulatory ; legislative** and other developments ~~.~~ ~~and these~~ **These** changes may ~~also in turn~~ **also in turn** impair our ability to offer our existing or planned products and services and increase our cost of doing business **in various countries**. Our business performance and growth plans could be negatively affected if we are not able to develop and implement improvements in technology or respond effectively to the threat of digital disruption and other technological change such as AI. We depend in large part on our technology systems for conducting business, as well as for providing the data and analytics we use to manage our business. As a result, our business success is dependent on maintaining the effectiveness of existing technology systems and on continuing to develop and enhance technology systems that support our business processes and strategic initiatives in a cost and resource efficient manner, particularly as our business processes become more digital. We have a number of strategic initiatives involving investments in or partnerships with technology companies as part of our growth strategy, as well as investments in technology, including generative AI, and infrastructure to support our own systems. These investments may be costly and require significant capital expenditures, may not be profitable or may be less profitable than what we have experienced historically. In addition, investments in technology systems may not deliver the benefits or perform as expected, or may be replaced or become obsolete more quickly than expected, which could result in operational difficulties or additional costs. In some cases, we also depend on key vendors and partners to provide technology and other support for our strategic initiatives. If these vendors or partners fail to perform their obligations or otherwise cease to work with us, our ability to execute on our strategic initiatives could be adversely affected. If we do not keep up with technological changes or execute effectively on our strategic initiatives, our business and results of operations could be adversely impacted. In addition, to remain competitive in many of our business areas, we must anticipate and respond effectively to the threat of digital disruption and other technological change such as generative AI. The threat comes from traditional players, such as insurers, through disintermediation as well as from new entrants, such as technology companies, "Insurtech" start-up companies and others. In the past few years, there has been a substantial increase in private equity investments into these Insurtech companies. These players are focused on using technology and innovation, including AI, digital platforms, data analytics, robotics and blockchain, to simplify and improve the client experience, increase efficiencies, alter business models and effect other potentially disruptive changes in the industries in which we operate. We are actively investing in generative AI tools. While our internal generative AI tool, LenAI, was designed to meet our standards for data security and to address and mitigate the risks associated with this new technology, our use of generative AI in certain products ~~and~~ **services and operations** may present risks and challenges that remain uncertain due to the relative novelty of this technology. These risks may include **operational disruptions or failures, reputational harm,** enhanced governmental or regulatory scrutiny, litigation or ethical concerns. **The models underlying AI tools may be incorrectly or inadequately designed or implemented and trained on, or otherwise use, data or algorithms that are (and the output generated by such AI tools also may be) biased, unethical, discriminatory, incomplete, inaccurate, misleading or poor-quality, any of which may not be easily detectable. To the extent that we do not have sufficient rights to use the data used in or output generated by such AI tools, we may be subject to litigation by holders of third-party intellectual property, privacy, publicity, contractual or other rights. If any of our employees, contractors, consultants, vendors or service providers use any third-party AI powered software in connection with our business or the services they provide to us, it may lead to the inadvertent disclosure or incorporation of our confidential information into publicly available training sets, which may impact our ability to realize the benefit of, or adequately maintain, protect and enforce our intellectual property or confidential information, harming our competitive position and business. In addition, the use of AI by other companies has resulted in, and our use of AI may in the future result in, data incidents and cybersecurity breaches.** While we ~~are~~ **have implementing implemented** certain mitigation measures and governance **related** to the proliferation of AI tools, these measures may be inadequate or may not ~~meet~~ **satisfy** a growing number of legal and regulatory requirements related to AI ~~.~~ **Moreover, if we are perceived to exaggerate the effectiveness, safety or ethical design of AI systems, this could lead to regulatory enforcement, litigation or reputational harm. Any misrepresentation, intentional or unintentional, of our AI-related capabilities or initiatives could also erode trust among clients and regulators. There can be no assurance that our use of AI will enhance our products, services or operations or otherwise result in our intended outcomes.** Competitive Risks The loss of members of our senior management team or other key colleagues, or if we are unsuccessful in our efforts to attract, retain and develop talent, could have a material adverse effect on our business. We rely upon the contributions of our senior management team to establish and implement our business strategy and to manage the future growth of our business. We may be unable to retain them, particularly if we do not offer employment terms that are competitive with the rest of the labor market. The loss of any of the senior management team could limit our ability to successfully execute our business strategy or adversely affect our ability to retain existing and attract new clients. Moreover, we could be adversely affected if we fail to adequately plan for the succession of members of our senior management team or if our succession plans do not operate effectively. Across all of our businesses, our colleagues are critical to developing and retaining client relationships as well as performing the services on which our revenues are earned. It is therefore important for us to attract, incentivize and retain significant revenue-producing employees and the key managerial and other professionals who support them. We face numerous challenges in this regard, including the intense competition for talent, which has accelerated in recent years. Such challenges

include the increased mobility of colleagues in light of more flexible working models, market dislocation resulting from proposed and actual combinations in the industry, raids by competitors, and fostering an inclusive and diverse workplace. Losing colleagues who manage or support substantial client relationships or possess substantial experience or expertise could adversely affect our ability to secure and complete client engagements, which could adversely affect our results of operations. If a key employee were to join an existing competitor or form a competing company, some of our clients could choose to use the services of that a competitor instead of our services. If a colleague joins us from a competitor and is subject to enforceable restrictive covenants, we may not be able to secure client engagements or maximize the colleague's potential. In addition, regulation or legislation impacting the workforce, such as the proposed U. S. Federal Trade Commission rule regarding noncompete clauses, may lead to increased uncertainty and competition for talent. Failure to maintain our corporate culture ; particularly in a hybrid work environment, could damage adversely affect our business and reputation. We strive to foster a culture in which our colleagues act with integrity and feel comfortable speaking up about potential misconduct. We are a people business, and our ability a well- defined and consistently reinforced corporate culture, starting with a strong " tone from the top , " is critical to ensuring compliance with laws and regulations, attract attracting and retain retaining colleagues top talent and maintaining the trust of our clients is dependent upon our commitment to an inclusive and diverse workplace, trustworthiness, ethical business partners practices and other qualities. Our colleagues are the cornerstone of this culture, and acts of misconduct by any colleague, and particularly by senior management, could erode trust and confidence and damage our reputation among existing and potential clients and other stakeholders. Remote As a multinational company operating across many geographies, failure to effectively align our workforce with our core values and hybrid work arrangements ethical principles may impair our ability to achieve our strategic objectives , particularly following the COVID-19 pandemic, may also negatively impact our ability as we execute operational model changes and integrate acquisitions. If we fail to maintain and promote our corporate culture, there as we believe being together is integral to promoting an increased risk of unethical behavior our- or culture-regulatory violations, which could result in legal penalties, reputational damage and financial harm . Increasing scrutiny and changing laws and expectations from regulators, investors, clients and our colleagues with respect to our environmental, social and governance (ESG) practices and disclosure may impose additional costs on us or expose us to new or additional risks. There is increased-continued focus, including from governmental organizations, regulators (including the SEC in the U. S.-), investors, colleagues and clients, on ESG and sustainability issues such as environmental stewardship, climate change, greenhouse gas emissions, inclusion and diversity, human rights, racial justice, pay equity, workplace conduct, cybersecurity and data privacy. The regulatory landscape related Negative public perception, adverse publicity or negative comments in social media could damage our reputation if we do not, or are not perceived to , adequately address these issues continues . Any harm to evolve, our reputation could impact colleague engagement and retention and the willingness of clients and our partners to do business with new us. Additionally, there has been increased regulatory focus on ESG and sustainability. For example, laws and reporting requirements introduced across various jurisdictions regulations related to ESG issues continue to evolve, including in the U. S., the U. K., the EU European Union (E. U.) and Australia . ; and these These laws and regulations may impose additional compliance or disclosure obligations on us. Inconsistent In particular, heightened demand for- or even conflicting requirements across jurisdictions , and scrutiny of, ESG and sustainable-related products, funds, investment strategies and advice has increased the risk that we could be perceived as, or accused of, making inaccurate or misleading statements, commonly referred to as " greenwashing " or that we have otherwise run afoul of regulation. Such perceptions or accusations could damage our reputation, result in litigation or regulatory enforcement actions, and adversely affect our business. Furthermore, perceptions of our efforts to achieve ESG goals or advance ESG and sustainable-related products, funds, investment strategies or advice may differ widely among also increase compliance challenges, add operational costs, or lead to stakeholders- stakeholder dissatisfaction and could present risks to our reputation and business, including litigation risk . As For example, in the U. S. there these has been increased legal scrutiny on inclusion and diversity-related programs and initiatives. Moreover, as ESG reporting requirements and standards continue to evolve , including with guidance from the International Sustainability Standards Board (ISSB) and the European Sustainability Reporting Standards (ESRS) under the Corporate Sustainability Reporting Directive (CSRD), we continue to evaluate and update our public disclosures in these areas, including refining our disclosure of metrics and sustainability goals in accordance with the guidance and our own ESG assessments and priorities. These disclosures, metrics and sustainability goals and any failure to accurately report or comply with federal, state or international ESG laws and regulations, or to achieve progress on our metrics and sustainability goals on a timely basis, or at all, may result in legal and regulatory proceedings against us and negatively impact our reputation. Implementation of our ESG initiatives also depends in part on third- party performance or data that is outside the Company's control. In addition, heightened regulatory scrutiny of ESG and sustainability- related products, funds, investment strategies and advice has increased the risk that we could be perceived as, or accused of, making inaccurate or misleading statements, or that we have otherwise run afoul of regulation. Such perceptions or accusations could damage our reputation, result in litigation or regulatory enforcement actions, and adversely affect our business. Organizations Organizations that provide information to investors on corporate governance and related matters have also developed ratings processes for evaluating companies on their approach to ESG matters, and unfavorable ratings of our company or our industries may lead to negative investor sentiment and the diversion of investment to other companies or industries, exclusion of our stock from ESG- oriented indices or investment funds or harm our relationships with regulators and the communities in which we operate . Moreover, public opinion and potential legal actions regarding ESG- related initiatives remain highly dynamic and can vary across stakeholders and geographies. Balancing these competing expectations globally is complex. The impact of new laws and regulations, negative public perception, adverse publicity or negative comments in social media could damage our reputation, and be costly to defend, if we do not, or are not perceived to, adequately address these issues. Any harm to our reputation could impact colleague engagement and

retention and the willingness of clients and our partners to do business with us. We face significant competitive pressures in each of our businesses, including from disintermediation, as our competitive landscape continues to evolve. As a global professional services firm, the Company faces competition in each of its businesses, and the competitive landscape continues to change and evolve. Our ability to compete successfully depends on a variety of factors, including the quality and expertise of our colleagues, our geographic reach, the sophistication and quality of our services, our pricing relative to competitors, our clients' ability to self-insure or use internal resources instead of consultants, and our ability to respond to changes in client demand and industry conditions. Any failure by us to design and execute operating model changes that capture opportunities and efficiencies at the intersections of our businesses and maximize the value we deliver to clients and stakeholders could have an adverse impact on our business. Additionally, some of our competitors may have greater financial resources, or may be better positioned to respond to technological and other changes in the industries we serve, and they may be able to compete more effectively. Furthermore, the competition for talent continues to accelerate. Across our Risk and Insurance Services segment, we operate in a variety of markets and face different competitive landscapes. In addition to the challenges posed by capital market alternatives to traditional insurance and reinsurance, we compete against a wide range of other insurance and reinsurance brokerage and risk advisory firms that operate on a global, regional, national or local scale for both client business and employee talent. In recent years, private equity sponsors have invested tens of billions of dollars into the insurance brokerage sector, transforming existing players and creating new ones to compete with large brokers. We also compete with insurance companies that market and service their insurance products directly to consumers and reinsurance companies that market and service their products directly to insurance companies, in each case without the assistance of brokers or other market intermediaries, and with various other companies that provide risk-related services or alternatives to traditional brokerage services, including those that rely almost exclusively on technological solutions or platforms. This competition is intensified by an often "syndicated" or "distributed" approach to the purchase of insurance and reinsurance brokerage services, where a client engages multiple brokers to service different portions of the client's account. In addition, third party capital providers have entered the insurance and reinsurance risk transfer market offering products and capital directly to our clients that serve as substitutes for traditional insurance. In our Consulting segment, we compete for business with numerous consulting firms and similar organizations, many of which also provide, or are affiliated with firms that provide, accounting, information systems, technology and financial services. Such competitors may be able to offer more comprehensive products and services to potential clients, which may give them a competitive advantage. Some of our competitors also may be able to invest more significant capital in technology and digital solutions. In certain sub-segments, we compete in highly fragmented markets or with start-ups that may be able to offer solutions at a lower price or on more favorable conditions. In addition, companies in the industries that we serve may seek to achieve economies of scale and other synergies by combining with or acquiring other companies. If two or more of our current clients merge, or consolidate or combine their operations, it may decrease the amount of work that we perform for these clients. We rely on a large number of vendors and other third parties to perform key functions of our business operations and to provide services to our clients. These vendors and third parties may act or fail to act in ways that could harm our business. We rely on a large number of vendors and other third parties, and in some cases subcontractors, to provide services, data and information such as technology, information security, funds transfers, business process management, and administration and support functions that are critical to the operations of our business. These third parties include correspondents, agents and other brokers and intermediaries, insurance markets, data providers, plan trustees, payroll service providers, software and system vendors, health plan providers, investment managers, custodians, risk modeling providers, and providers of human resource functions, such as recruiters. Many of these providers are located outside the U. S., which exposes us to business disruptions and political risks inherent when conducting business outside of the U. S. As we do not control many of the actions of these third parties, we are subject to the risk that their decisions or operations may adversely impact us and replacing these service providers could create significant delay in services or operations and additional expense. A failure by the third parties to (i) comply with service level agreements in a high quality and timely manner, particularly during periods of our peak demand for their services, (ii) maintain adequate internal controls that may impact our own financial reporting, or (iii) adequately maintain the confidentiality of any of our data or trade secrets or adequately protect or properly use other intellectual property to which they may have access, could result in economic and reputational harm to us. These third parties also face their own technology, operating, business and economic risks, and any significant failures by them, including the improper use or disclosure of our confidential client, employee, or Company information or failure to comply with applicable law, could cause harm to our reputation or otherwise expose us to liability. An interruption in or the cessation of service by any service provider as a result of systems failures, capacity constraints, non-compliance with legal, regulatory or contractual obligations, financial difficulties or for any other reason could disrupt our operations, impact our ability to offer certain products and services, and result in contractual or regulatory penalties, liability claims from clients or employees, damage to our reputation and harm to our business. Business Resiliency Risks Our inability to successfully recover should we experience a disaster or other business continuity or data recovery problem could cause material financial loss, loss of human capital, regulatory actions, reputational harm or legal liability. If we experience a local or regional disaster or other business continuity event, such as an earthquake, hurricane, flood, terrorist attack, pandemic, war or other geopolitical tensions, protests or riots, security breach, cyberattack (including manipulating the control systems of critical infrastructure), power loss or telecommunications failure, our ability to operate will depend, in part, on the continued availability of our personnel, our office facilities and the proper functioning of our computer, telecommunication and other related systems and operations. In such an event, we could experience operational challenges that could have a material adverse effect on our business. The risk of business disruption is more pronounced in certain geographic areas, including major metropolitan centers, like New York or London, where we have significant operations and approximately 3, 700-900 and 5, 700-800 colleagues in those respective locations, and in certain countries and regions, **such as India**, in which we operate **or are investing additional capabilities** that are subject to higher potential threat of terrorist attacks or military

conflicts. Our operations depend in particular upon our ability to protect our technology infrastructure against damage. If a business continuity event occurs, we could lose client or Company data or experience interruptions to our operations or delivery of services to our clients, which could have a material adverse effect. Such risks have increased significantly due to hybrid and remote work environments. A cyberattack or other business continuity event affecting us or a key vendor or other third party could result in a significant and extended disruption in the functioning of our information technology systems or operations or our ability to recover data, requiring us to incur significant expense to address and remediate or otherwise resolve such issues. For example, hackers have increasingly targeted companies by attacking internet-connected industrial control and safety control systems. An extended outage could result in the loss of clients and a decline in our revenues. In the worst case, any manipulation of the control systems of critical infrastructure may even result in the loss of life. We regularly assess and take steps to improve our existing business continuity, disaster recovery and data recovery plans and key management succession. However, a disaster or other continuity event on a significant scale or affecting certain of our key operating areas within or across regions, or our inability to successfully recover from such an event, could materially interrupt our business operations and result in material financial loss, loss of human capital, regulatory actions, reputational harm, damaged client relationships and legal liability. Our business disruption insurance may also not fully cover, in type or amount, the cost of a successful recovery in the event of such a disruption.

Acquisitions and Dispositions Risks We face risks when we acquire or dispose of businesses. We have a history of making acquisitions and investments, including a total of ~~80-86~~ in the period from ~~2019 to 2023~~ **2020 to 2024, including our recent acquisition of McGriff Insurance Services, LLC (" McGriff") and Gerolamo Holding S. À. R. L. (" Cardano")**. We may not be able to successfully integrate the businesses that we acquire into our own business, or achieve any expected cost savings or synergies from the integration of such businesses, **including McGriff and Cardano**. Subject to standard contractual protections, we may also be responsible for legacy liabilities of companies that we acquire. **Moreover, if we acquire a business operating in regions or industries subject to heightened regulatory scrutiny, we may face significant costs or risks in bringing their operations into compliance with applicable laws and our internal policies. Failure to address these compliance risks could result in regulatory enforcement actions, fines or damage to our reputation**. In addition, if in the future the performance of our reporting units or an acquired business varies from our projections or assumptions, or estimates about future profitability of our reporting units or an acquired business change, the estimated fair value of our reporting units or an acquired business could change materially and could result in an impairment of goodwill and other acquisition-related intangible assets recorded on our balance sheet or in adjustments in contingent payment amounts. Given the significant size of the Company's goodwill and intangible assets, an impairment could have a material adverse effect on our results of operations in any given period. We expect that acquisitions will continue to be a key part of our business strategy. Our success in this regard will depend on our ability to identify and compete for appropriate acquisition candidates and to finance and complete the transactions we decide to pursue on favorable terms with positive results. When we dispose of businesses, we may continue to be subject to certain liabilities of that business after its disposition relating to the prior period of our ownership and may not be able to negotiate for limitations on those liabilities. We are also subject to the risk that the sales price is less than the amount reflected on our balance sheet.

Financial Risks If we are unable to collect our receivables, our results of operations and cash flows could be adversely affected. Our business depends on our ability to obtain payment from our clients of the amounts they owe us for the work we perform. As of December 31, ~~2023~~ **2024**, our receivables for our commissions and fees were approximately \$ ~~6.5-8~~ billion, or approximately one-quarter of our total annual revenues, and portions of our receivables are increasingly concentrated in certain businesses and geographies. Macroeconomic or geopolitical conditions, such as a slower economic growth or recession, the war in Ukraine and the ~~escalating~~ conflict throughout the Middle East, inflationary pressures or supply chain challenges, could result in financial difficulties for our clients, which could cause clients to delay payments to us, request modifications to their payment arrangements that could increase our receivables balance or default on their payment obligations to us. We may not be able to obtain sufficient financing on favorable terms. The maintenance and growth of our business, including our ability to finance acquisitions, the payment of dividends and our ability to make share repurchases rely on our access to capital, which depends in large part on cash flow generated by our business and the availability of equity and debt financing. Certain of our businesses also rely on financings by the Company to fund the underwriting of their client's debt and equity capital raising transactions. There can be no assurance that our operations will generate sufficient positive cash flow to finance all of our capital needs or that we will be able to obtain equity or debt financing on favorable terms, particularly in an environment of rising interest rates. In addition, our ability to obtain financing will depend in part upon prevailing conditions in credit and capital markets, which are beyond our control. Our defined benefit pension plan obligations could cause the Company's financial position, earnings and cash flows to fluctuate. Our defined benefit pension obligations and the assets set aside to fund those obligations are sensitive to certain changes in the financial markets. Any such changes may result in increased pension expense or additional cash payments to fund these plans. The Company has significant defined benefit pension obligations to its current and former employees, totaling approximately \$ ~~12-11~~ **2-4** billion, and related plan assets of approximately \$ ~~13-12~~ **5-6** billion, at December 31, ~~2023~~ **2024 on a in accordance with** U. S. GAAP basis. The Company's policy for funding its defined benefit pension plans is to contribute amounts at least sufficient to meet the funding requirements set forth by law. In the U. S., contributions to these plans are based on ERISA guidelines. Outside the ~~United States~~ **U. S.**, contributions are generally based on statutory requirements and local funding practices, which may differ from measurements in accordance with U. S. GAAP. In the U. K., for example, the assumptions used to determine pension contributions are the result of legally-prescribed negotiations between the Company and the plan trustees. Currently, the use of these assumptions results in a lower funded status than determined in accordance with U. S. GAAP and may result in contributions irrespective of the U. S. GAAP funded status. The financial calculations relating to our defined benefit pension plans are complex. Pension plan assets could decrease as the result of poor future asset performance. In addition, the estimated return on plan assets would likely be impacted by changes in the interest rate environment and other factors, including equity

valuations, since these factors reflect the starting point used in the Company's projection models. For example, a reduction in interest rates may result in a reduction in the estimated return on plan assets. Also, pension plan liabilities, periodic pension expense and future funding amounts could increase as a result of a decline in the interest rates we use to discount our pension liabilities, longer lifespans than those reflected in our mortality assumptions, changes in investment markets that result in lower expected returns on assets, actual investment return that is less than the expected return on assets, adverse changes in laws or regulations and other variables. Finally, changes in the aggregated, smoothed asset returns as future years replace prior years, has an impact on both the level and the volatility of pension expense. While we have taken steps to mitigate the impact of pension volatility on our earnings and cash funding requirements, these strategies may not be successful. Accordingly, given the magnitude of our worldwide pension plans, variations in or reassessment of the preceding or other factors or potential miscalculations relating to our defined benefit pension plans could cause significant fluctuation from year to year in our earnings and cash flow, as well as our pension plan assets and liabilities, and may result in increased levels of contributions to our pension plans. Our significant non- U. S. operations expose us to exchange rate fluctuations and various risks that could impact our business. Approximately 53-52% of our total revenue reported in 2023-2024 was from business outside of the U. S. We are subject to exchange rate movement because we must translate the financial results of our foreign subsidiaries into U. S. dollars and also because some of our subsidiaries receive revenue other than in their functional currencies. Exchange rate movements may change over time, and they could have a material adverse impact on our financial results and cash flows reported in U. S. dollars. For additional discussion, see "Market Risk and Credit Risk- Foreign Currency Risk" in Part II, Item 7A ("Quantitative and Qualitative Disclosures about Market Risk") of this report. Our quarterly revenues and profitability may fluctuate significantly. Quarterly variations in revenues and operating results may occur due to several factors. These include: • the number of client engagements during a quarter; • the possibility that clients may decide to delay or terminate a current or anticipated project as a result of factors unrelated to our work product or progress; • fluctuations in capacity and utilization rates and clients' ability to terminate engagements without penalty; • our net colleague hires and related compensation and benefits expense; • potential limitations on the clients or industries we serve resulting from increased regulation or changing stakeholder expectations on ESG issues; • the impact of changes in accounting standards or in our accounting estimates or assumptions; • the impact on us or our clients of changes in legislation, regulation and legal guidance or interpretations in the jurisdictions in which we operate, in particular particularly in the U. S. as a result of increased regulatory activity and enforcement the shift in the presidential administration; • seasonality due to the impact of regulatory deadlines, policy renewals and other timing factors to which our clients are subject; • the success of our acquisitions or investments; • occurrence of any significant natural disaster or other insured events including any potential reputational harm to the insurance industry following such event; • macroeconomic factors such as changes in foreign exchange rates, interest rates and global public and private capital markets, particularly in the case of Mercer, where fees in its investments business and certain other business lines are derived from the value of assets under management, advisement or administration; and • general economic conditions, including factors beyond our control affecting economic conditions such as global health crises or pandemics, severe weather, climate change, geopolitical unrest such as the war in Ukraine and the escalating conflict throughout the Middle East, protests and riots or other catastrophic events, since our results of operations are directly affected by the levels of business activity of our clients, which in turn are affected by the level of economic activity in the industries and markets that they serve. A significant portion of our total operating expenses is relatively fixed in the short term. Therefore, a variation in the number of client assignments or in the timing of the initiation or the completion of client assignments can cause significant variations in quarterly operating results for these businesses. Credit rating downgrades would increase our financing costs and could subject us to operational risk. Currently, the Company's senior debt is rated A- by S & P, A3 by Moody's and A- by Fitch. The Company's short-term debt is currently rated A- 2 by S & P, P- 2 by Moody's, and F- 2 by Fitch. The Company carries a Stable outlook with S & P, Moody's and Fitch. If we need to raise capital in the future (for example, in order to maintain adequate liquidity, fund maturing debt obligations or finance acquisitions or other initiatives), credit rating downgrades would increase our financing costs, and could limit our access to financing sources. A downgrade to a rating below investment-grade could result in greater operational risks through increased operating costs and increased competitive pressures. Our current debt level could adversely affect our financial flexibility. At As of December 31, 2023-2024, we had total consolidated debt outstanding of approximately \$ 13-19. 5-9 billion. The level of debt outstanding could adversely affect our financial flexibility by reducing our cash flows and our ability to use cash from operations for other purposes, including working capital, dividends to shareholders, share repurchases, acquisitions, capital expenditures and general corporate purposes. In addition, we are subject to risks that, at the time any of our outstanding debt matures, we will not be able to retire or refinance the debt on terms that are acceptable to us. The current U. S. tax regime has provisions which have unintended consequences and may also impact our tax rate in varying degrees based on where our global income is earned. Our effective tax rate may fluctuate in the future as a result of the current U. S. tax regime and the continuing issuance of interpretive guidance related to the operations of U. S.- based multinational corporations. These include significant provisions in U. S. income tax law that may have a meaningful impact on our income tax expense and require significant judgments and estimates in interpretation and calculations. Current tax legislation includes, among other provisions, limitations on the deductibility of net interest expense, a minimum tax on most non- U. S. income called Global Intangible Low- Taxed Income ("GILTI"), and the Base Erosion and Anti- Abuse Tax ("BEAT"). In addition, a recently enacted book minimum tax could increase the impact of these provisions on our income tax expense. Given the significant complexity of the rules, and the potential for additional guidance from the U. S. Treasury, the Securities and Exchange Commission, the Financial Accounting Standards Board or other regulatory authorities, recognized impacts in future periods could be significantly different from our current estimates. Such uncertainty may also result in increased scrutiny from, or disagreements with, tax authorities. As a U. S.- domiciled company, any such increases would likely have a disproportionate impact on us compared to our foreign- based competitors. Global Operations We are exposed to multiple risks associated with

the global nature of our operations. We conduct business globally. In 2023-2024, approximately 53-52% of the Company's total revenue was generated from operations outside the U. S., and over one-half of our employees were located outside the U. S. In addition, we conduct our operations through four separate businesses. Potential conflicts of interest may arise across our businesses given the significant volume of our engagements. The geographic breadth of our activities also subjects us to significant legal, economic, operational, market, compliance and reputational risks. These include, among others, risks relating to: • economic and political conditions in the countries in which we operate; • client concentration in certain high-growth countries in which we operate; • the length of payment cycles and potential difficulties in collecting accounts receivable; • unexpected increases in taxes or changes in U. S. or foreign tax laws, rulings, policies or related legal and regulatory interpretations, including recent changes to the U. K. statutory rate; • the implementation of the Organization for Economic Cooperation and Development (OECD) international tax framework, including the implementation of the Pillar 2 minimum tax regime by key jurisdictions in 2024 and the Pillar 1 profit reallocation regime, which could have potentially resulting in an adverse effect on our effective tax rate, tax payments and results of operations, particularly as key jurisdictions adopt these changes, either partially or in full, alongside potential shifts in tax laws in response to such implementation; • international initiatives to require multinational enterprises, like ours, to calculate and report profitability on a country-by-country basis, which could increase scrutiny by, or cause disagreements with, foreign tax authorities; • potential transfer pricing-related tax exposures that may result from the flow of funds among our subsidiaries and affiliates in the various jurisdictions in which we operate; • unexpected reassessment by tax authorities of interpretations of existing rules which may require companies to defend previously accepted positions and may create both new and prior-year exposures; • litigation arising from ongoing and future controversies with tax authorities; • permanent establishments created due to colleagues traveling to and doing work in certain countries where the Company has no presence, or living in such countries and working remotely post-pandemic, which are not properly compensated through transfer pricing; • our ability to obtain dividends or repatriate funds from our non-U. S. subsidiaries, including as a result of the imposition of currency controls and other government restrictions on repatriation in the jurisdictions in which our subsidiaries operate, fluctuations in foreign exchange rates and the imposition of withholding and other taxes on such payments; • geopolitical tensions, such as the war in Ukraine and the escalating conflict throughout the Middle East, in countries where we operate, international hostilities, international trade disputes, terrorist activities, natural disasters, pandemics, and infrastructure disruptions; • local investment or other financial restrictions that foreign governments may impose; • potential lawsuits, investigations, market studies, reviews or other activity by foreign regulatory or law enforcement authorities or legislatively appointed commissions, which may result in potential modifications to our businesses, related private litigation or increased scrutiny from U. S. or other regulators; • potential costs and difficulties in complying with a wide variety of foreign laws and regulations (including tax systems) administered by foreign government agencies, some of which may conflict with U. S. or other sources of law; • potential costs and difficulties in complying, or monitoring compliance, with foreign and U. S. laws and regulations that are applicable to our operations abroad, including trade sanctions laws relating to countries such as Afghanistan, Belarus, Cuba, Iran, North Korea, Russia, Syria, Ukraine (Russia-controlled territories) and Venezuela, anti-corruption laws such as the U. S. Foreign Corrupt Practices Act and the U. K. Bribery Act 2010; • limitations or restrictions that foreign or U. S. governments and regulators may impose on the products or services we sell, the methods by which we sell our products and services and the manner in which and the amounts we are compensated; • potential limitations or difficulties in protecting our intellectual property in various foreign jurisdictions; • limitations that foreign governments may impose on the conversion of currency or the payment of dividends or other remittances to us from our non-U. S. subsidiaries; • engaging and relying on third parties to perform services on behalf of the Company; and • potential difficulties in monitoring employees in geographically dispersed locations.

RISKS RELATING TO OUR RISK AND INSURANCE SERVICES SEGMENT Our Risk and Insurance Services segment, conducted through Marsh and Guy Carpenter, represented 62-63% of the Company's total revenue in 2023-2024. Our business in this segment is subject to particular risks. Results in our Risk and Insurance Services segment may be adversely affected by a general decline in economic activity. Demand for many types of insurance and reinsurance generally rises or falls as economic growth expands or slows. This dynamic affects the level of commissions and fees generated by Marsh and Guy Carpenter. To the extent our clients become adversely affected by declining business conditions, they may choose to limit their purchases of risk services and insurance and reinsurance coverage, as applicable, which would adversely impact our commission revenue and other revenue based on premiums placed and services provided by us. Also, the insurance they seek to obtain through us may be impacted by changes in their assets, property values, sales or number of employees, which may reduce our commission revenue, and they may decide not to purchase our risk advisory or other services, which would inhibit our ability to generate fee revenue. Moreover, insolvencies and combinations associated with an economic downturn, especially insolvencies and combinations in the insurance industry, could adversely affect our brokerage business through the loss of clients or by limiting our ability to place insurance and reinsurance business, as well as our revenues from insurers. Guy Carpenter is especially susceptible to this risk given the limited number of insurance company clients and reinsurers in the marketplace. Volatility or declines in premiums and other market trends may significantly impede our ability to grow revenues and profitability. A significant portion of our Risk and Insurance Services revenue consists of commissions paid to us out of the premiums that insurers and reinsurers charge our clients for coverage. We do not determine the insurance premiums on which our commissions are generally based. Our revenues and profitability are subject to change to the extent that premium rates fluctuate or trend in a particular direction. The potential for changes in premium rates is significant, due to the normal cycles of pricing in the commercial insurance and reinsurance markets. As traditional insurance companies continue to rely on non-affiliated brokers or agents to generate premium, those insurance companies may seek to reduce their expenses by lowering their commission rates. The reduction of these commission rates, along with general volatility or declines in premiums, may significantly affect our revenue and profitability. Because we do not determine the timing or extent of premium pricing changes, it is difficult to accurately forecast our commission revenues, including whether they will

significantly decline. As a result, we may have to adjust our plans for future acquisitions, capital expenditures, dividend payments, loan repayments and other expenditures to account for unexpected changes in revenues, and any decreases in premium rates may adversely affect the results of our operations. In addition to movements in premium rates, our (and Mercer's Health business's) ability to generate premium-based commission revenue may be challenged by disintermediation and the growing availability of alternative methods for clients to meet their risk-protection needs. This trend includes a greater willingness on the part of corporations to self-insure, the expanded use of captive insurers, and the presence of capital markets-based solutions for traditional insurance and reinsurance needs. Further, the profitability of our Risk and Insurance Services segment depends in part on our ability to be compensated for the analytical services and other advice that we provide, including the consulting and analytics services that we provide to insurers. If we are unable to achieve and maintain adequate billing rates for all of our services, our margins and profitability could decline. Adverse legal developments and future regulations concerning how intermediaries are compensated by insurers or clients, as well as allegations of anti-competitive behavior or conflicts of interest, could have a material adverse effect on our business, results of operations and financial condition. The ways in which insurance intermediaries are compensated receive scrutiny from regulators in part because of the potential for anti-competitive behavior and conflicts of interest. The vast majority of the compensation that Marsh receives is in the form of retail fees and commissions that are paid by the client or paid from premium that is paid by the client. The amount of other compensation that we receive from insurance companies, separate from retail fees and commissions, has increased in the last several years, both on an underlying basis and through acquisition and represented approximately 6 % of Marsh's revenue in **2023-2024**. This other compensation includes payment for (i) consulting and analytics services provided to insurers; (ii) administrative and other services provided to insurers (including underwriting services and services relating to the administration and management of quota shares, panels and other facilities); and (iii) contingent commissions, primarily at MMA and outside the U. S., paid by insurers based on factors such as volume or profitability. These other revenue streams present potential regulatory, litigation and reputational risks that may arise from alleged anti-competitive behavior or conflicts of interest, (including those arising from Guy Carpenter's role as intermediary and advisor for insurance companies), and future changes in the regulatory environment may impact our ability to collect such revenue. Adverse regulatory, legal or other developments could have a material adverse effect on our business and expose the Company to negative publicity and reputational harm.

RISKS RELATING TO OUR CONSULTING SEGMENT Our Consulting segment, conducted through Mercer and Oliver Wyman Group, represented **38-37%** of our total revenue in **2023-2024**. Our businesses in this segment are subject to particular risks. Mercer's Wealth business is subject to a number of risks, including risks related to public and private capital market fluctuations, third-party asset managers and custodians, operations and technology **risks, trading and execution** risks, conflicts of interest, ESG and greenwashing, asset performance and regulatory compliance, that, if realized, could result in significant damage to our business. Mercer's Investments business provides clients with digital tools, investment consulting and investment management services. Mercer's Investments business is subject to a number of risks, including risks related to litigation (both by clients and by plan participants, particularly **as when we increasingly act in a fiduciary capacity**), liquidity and market volatility, an inability to obtain contractual limitations of liability for errors & omissions in certain jurisdictions or parts of our business, third-parties, our operations and technology (including the use of AI), trading **and execution** errors, conflicts of interest, asset performance and regulatory compliance and scrutiny, which could arise in connection with these offerings. For example, Mercer's manager research or due diligence on an asset manager may fail to uncover material deficiencies or fraud that could result in investment losses to a client. There is a risk that Mercer will fail to properly or timely implement **or execute** a client's investment policy or **direction-strategy or instruction**, which could cause an incorrect or untimely allocation of client assets among asset classes, asset managers, or strategies **or result in a trading error**. Mercer may also be perceived as making inaccurate or misleading statements regarding the investment strategies of our offerings or investments with respect to ESG or sustainability, commonly referred to as "greenwashing," or recommending certain asset managers to clients or offering delegated solutions **to an investment consulting a potential or existing** client, solely to enhance its own compensation or due to other **perceived** conflicts of interest. Asset classes may perform poorly, or asset managers may underperform their benchmarks, due to poor market performance, a downturn in the global markets, negligence or other reasons, resulting in poor returns or loss of client assets. Changes in the value of equity, debt, currency, real estate, commodities, alternatives or other asset classes, in particular as a result of a downturn in the global markets, could cause the value of assets under management or advisement, and the fees earned by Mercer to decline. Mercer or its clients may be subject to claims or class action litigation relating to advice given or investment decisions made by plan sponsors and plan fiduciaries, particularly relating to 401 (k) plans in the U. S. or pension schemes in the U. K. These risks, if realized, could result in significant liability and damage our business. **Our businesses are subject to a number of risks related to the U. S. healthcare industry, including risks related to healthcare regulation and reputational damage from negative publicity. Mercer, MMA and MMB help public and private sector employers design and manage employee health and welfare programs. Their services include plan design, brokering of insurance programs, administration and other consulting and specialty services. The healthcare industry, inclusive of health insurance, is regulated by federal, state and local governments in the U. S., and by regulators and governments in other countries where we do business. The laws and rules governing the healthcare industry and interpretations of those laws and rules are subject to frequent and often unpredictable change. For example, legislation or regulatory action that has the impact of disincentivizing U. S. companies from offering employer-sponsored health insurance could ultimately reduce the revenue we receive when consulting on and broking these policies on behalf of our corporate clients. Legislation seeking to regulate pharmacy benefit management services introduced or enacted at the federal or state level could impact the compensation structure and how much we are paid where we advise clients on prescription drug coverage. Changes to U. S. government health programs, like Medicaid, could also impact our consulting and ancillary services for government clients that manage these programs. Moreover,**

the health care industry is regularly subject to negative publicity, including as a result of governmental investigations, adverse media coverage and political debate concerning industry regulation. Negative publicity may adversely affect our business and damage our reputation, and expose us to unexpected or unwarranted regulatory scrutiny, including as a result of the revenue our businesses receive from healthcare- related services including our consulting advice to clients from different areas of the healthcare industry . Revenues for the services provided by our Consulting segment may decline for various reasons, including as a result of changes in economic conditions, the value of equity, debt and other asset classes, our clients' or an industry' s financial condition or government regulation or an accelerated trend away from actively managed investments to passively managed investments. Global economic conditions, including slower GDP growth or recession, inflationary pressure and foreign exchange rate volatility, may negatively impact businesses and financial institutions. Many of our clients, including financial institutions, corporations, government entities and pension plans, have reduced expenses, including amounts spent on consulting services, and used internal resources instead of consultants during difficult economic periods. The evolving needs and financial circumstances of our clients may reduce demand for our consulting services and could adversely affect our revenues and profitability. If the economy or markets in which we operate experience weakness or deteriorate, our business, financial condition and results of operations could be materially and adversely affected. If our clients reduce their headcounts, they will have fewer employee lives covered under their health plans, which may reduce premiums and the commission or supplemental compensation Mercer may receive. In addition, some of Mercer' s Investments business generate fees based upon the value of the clients' assets under management, advisement or administration. Changes in the value of equity, debt, currency, real estate, commodities, alternatives or other asset classes could cause the value of assets under management, advisement or administration, and the fees received by Mercer, to decline. Such changes could also cause clients to withdraw funds from Mercer' s Investments business in favor of other investment service providers. In either case, our business, financial condition and results of operations could be materially adversely affected. Mercer' s Investments business also could be adversely affected by an accelerated shift away from actively managed investments to passively managed investments with associated lower fees **, as well as fee compression from the competitive environment** . Further, revenue received by Mercer as investment manager to the majority of the Mercer- managed investment funds is reported in accordance with U. S. GAAP on a gross basis rather than a net basis, with sub- advisor fees reflected as an expense. Therefore, the reported revenue for these offerings does not fully reflect the amount of net revenue ultimately attributable to Mercer. Demand for many of Mercer' s benefits services is affected by government regulation and tax laws, rulings, policies and interpretations, which drive our clients' needs for benefits- related services. Significant changes in government regulations affecting the value, use or delivery of benefits and human resources programs, including changes in regulations relating to health and welfare plans, defined contribution plans or defined benefit plans, may adversely affect the demand for or profitability of Mercer' s services. Factors affecting defined benefit pension plans and the services we provide relating to those plans could adversely affect Mercer. Mercer currently provides plan sponsors, plan trustees, multi- employer and public entity clients with actuarial, consulting and administration services relating to defined benefit pension plans. The nature of our work is complex. Many clients, particularly in the public sector, have sizeable pension deficits and are subject to impact from volatility in the global markets and interest rate fluctuations. A number of Mercer' s clients have frozen or curtailed their defined benefit plans and have moved to defined contribution plans resulting in reduced revenue for Mercer' s retirement business. These developments, fee compression pressures, and a continued or accelerated rate of decline in revenues for our defined benefit pension plans business could adversely affect Mercer' s business and operating results. In addition, our actuarial services involve numerous assumptions and estimates regarding future and contingent events, including interest rates used to discount future liabilities, estimated rates of return for a plan' s assets, healthcare cost trends, salary projections and participants' life expectancies. Mercer' s consulting services involve the drafting and interpretation of trust deeds and other complex documentation governing pension plans. Mercer' s administration services include calculating benefits within complicated pension plan structures. Mercer' s investments services include investment advice and management relating to defined benefit pension plan assets intended to fund present and future benefit obligations. Clients dissatisfied with our services have brought, and may bring, significant claims against us, particularly in the U. S. and the ~~United Kingdom~~ **U. K.** Additionally, a rapid rise in interest rates could result in higher defined benefit pension plan funding levels. In some markets, this could accelerate clients' desire to conduct a buyout or third- party risk transfer. Such a transaction could result in additional short- term revenue for Mercer to the extent we advise the client on the transaction, but a loss in longer term recurring revenue related to the plan. The profitability of our Consulting businesses depends in part on ensuring that our consultants maintain adequate utilization rates (i. e., the percentage of our consultants' working hours devoted to billable activities). Our utilization rates are affected by a number of factors, including: • general economic conditions; • our ability to transition consultants promptly from completed projects to new assignments, and to engage newly- hired consultants quickly in revenue- generating activities; • our ability to continually secure new business engagements, particularly because a portion of our work is project- based rather than recurring in nature; • our ability to forecast demand for our services and thereby maintain appropriate headcount in each of our geographies and workforces; • our ability to retain key colleagues and consulting professionals; • unanticipated changes in the scope of client engagements; • the potential for conflicts of interest that might require us to decline client engagements that we otherwise would have accepted; • our need to devote time and resources to sales, training, professional development and other non- billable activities; and • the potential disruptive impact of acquisitions and dispositions. If the utilization rate for our consulting professionals declines, our revenues, profit margin and profitability could decline. In addition, the profitability of our Consulting businesses depends in part on the prices we are able to charge for our services. The prices we charge are affected by a number of factors, including: • clients' perception of our ability to add value through our services; • market demand for the services we provide; • our ability to develop new services and the introduction of new services by competitors; • the pricing policies of our competitors; and • the extent to which our clients develop in- house or other capabilities to perform the services that they might otherwise purchase from us. If we are unable to

achieve and maintain adequate billing rates for our services, our profit margin and profitability could decline.