# Market Trends 2020/21: Risk Factors

**A Practical Guidance® Practice Note by**
**Christina Thomas and Candace Jackson, Mayer Brown LLP**

Christina Thomas
Mayer Brown LLP

This practice note focuses on recent market trends in risk factor disclosure required in U.S. Securities and Exchange Commission (SEC) filings and provides recent risk factor disclosure examples, covering COVID-19, Brexit, London Interbank Offered Rate (LIBOR) cessation, cybersecurity, and China-based issuers. Additionally, this practice note discusses recent amendments to the description of the risk factor disclosure requirement, and how the amendments to the rule may affect risk factor disclosure going forward.

For additional practical guidance on risk factors, see Top 10 Practice Tips: Risk Factors and Risk Factor Drafting for a Registration Statement. For other market trends articles covering various capital markets and corporate governance topics, see Market Trends.

## Disclosure Requirement

The risk factor disclosure requirement is contained in Item 105 of Regulation S-K (17 C.F.R. § 229.105). It requires, in relevant part, companies to disclose: "a discussion of the material factors that make an investment in the registrant or offering speculative or risky."

## Filings Requiring Risk Factor Disclosure

Risk factor disclosure appears in SEC filings where the form being filed requires a risk factor section compliant with Item 105 of Regulation S-K, such as annual reports on Form 10-K, quarterly reports on Form 10-Q, and registration statements under the Securities Act of 1933 and the Securities Exchange Act of 1934.

For additional guidance on Form 10-K and Form 10-Q, see Form 10-K Drafting and Review, Form 10-Q Drafting and Review, Form 10-K Form Check: Checklist, and Form 10-Q Form Check: Checklist.

## Location of the Disclosure

Item 105(b) of Regulation S-K dictates that in a registration statement, risk factor disclosure must appear immediately after the summary section required by Item 503 of Regulation S-K. Item 105(b) further provides that if the filing does not contain a summary section, "the risk factor section must immediately follow the cover page of the prospectus or the pricing information section that immediately follows the cover page."

Form 10-K requires risk factor disclosure in Item 1A of Part I and Form 10-Q requires risk factor disclosure in Item 1A of Part II. Both Forms 10-K and 10-Q provide that smaller reporting companies are not required to provide risk factors in those forms.

# Recent Amendments Made in Response to Risk Factor Trends

The SEC adopted significant changes to the risk factor disclosure requirements in Item 105 of Regulation S-K that became effective on November 9, 2020. Specifically, the amendments require:

- Summary risk factor disclosure of two pages or less if the risk factor section in the filings exceeds 15 pages
- Disclosure of material risk factors (Item 105 previously required disclosure of the registrant's "most significant factors that make an investment in the registrant or offering speculative or risky" (emphasis added)) –and–
- Organization of risk factors under relevant headings—in addition to the subcaptions that the rules already require (Any risk factors that would be generally applicable to any company or any investment of securities must be disclosed at the end of the risk factor section in the filing under a separate heading.)

The impetus for the changes was based, in part, on trends such as the generic nature and increased length of risk factor disclosures in public company filings in recent years. The amendments are intended to encourage more tailored, company-specific disclosure.

Despite the amendments, tension may continue to exist between the SEC's goal of reducing the prevalence of lengthy, boilerplate risk factor disclosure and companies' decisions to include generic risks to avoid the potential for litigation if, in the future, a negative event should occur for which a corresponding risk factor was not included.

In the adopting release for the new amendments, the SEC estimated that absent changes made to future filings in response to the new requirements, approximately 40% of current filers would need to provide summary risk factor disclosure.

# Risk Factor Disclosure Examples

The disclosure trends covered in this practice note were precipitated by either recent macro-level events affecting a large number of public companies or the SEC and the SEC Division of Corporation Finance staff's increased attention to particular issues affecting a large number of public companies. Below are recent examples of risk factor disclosure relating to the following risks:

- COVID-19
- Brexit
- LIBOR cessation
- Cybersecurity
- China-based issuers

## Risk Factor Disclosure Relating to COVID-19 Risk

The SEC has been closely monitoring how companies disclose the effects and risks of COVID-19 on their businesses, financial condition, and results of operations. On April 8, 2020, SEC Chairman Clayton and Division of Corporation Finance Director Hinman published a statement entitled "The Importance of Disclosure – For Investors, Markets and Our Fight Against COVID-19." This public statement set forth expectations and provided guidance for companies entering earnings season in the early days of the global pandemic. Detailed guidance was also provided in CF Disclosure Guidance Topic No. 9 and CF Disclosure Guidance Topic No. 9A. In those publications, the SEC staff emphasized the need for companies to "provide disclosures that allow investors to evaluate the current and expected impact of COVID-19 through the eyes of management and to proactively revise and update disclosures as facts and circumstances change." Companies have disclosed the risks and impact of COVID-19 not only in risk factors related specifically to COVID-19, but have also disclosed COVID-19-related impacts in other risk factors, including the risks of global economic downturn, changes in consumer tastes and spending, the ability of customers and suppliers to meet their obligations to the issuers and third parties, and cybersecurity and data privacy risk. Below are several examples of how companies have disclosed COVID-19 risk.

### *Example 1*

***"The COVID-19 pandemic has affected how we and our customers are operating our respective businesses, and the duration and extent to which this will impact our future results of operations and our overall financial performance remains uncertain.***

A novel strain of coronavirus (COVID-19) was first identified in late calendar year 2019 and subsequently declared a pandemic by the World Health Organization in March 2020. The long-term impacts, if any, of the global COVID-19 pandemic on our business are currently unknown. We are conducting business as usual with modifications to employee travel, employee work locations, and cancellation of certain marketing events, among other modifications. We will continue to actively monitor

the situation and may take further actions that alter our business operations as may be required by federal, state or local authorities or that we determine are in the best interests of our employees, customers, partners, suppliers and stockholders. It is not clear what the potential long-term effects of any such alterations or modifications may have on our business, including the effects on our customers and prospects.

We have observed other companies, including customers and partners, taking precautionary and preemptive actions to address the COVID-19 pandemic. Such companies may take further actions that alter their normal business operations if there are future spikes of COVID-19 infections resulting in additional government mandated shutdowns. The conditions caused by the COVID-19 pandemic have adversely affected our customers' willingness to purchase our products and delayed prospective customers' purchasing decisions. The impacts of the global COVID-19 pandemic on the broader global economy have been swift, dramatic and unpredictable. The latency and duration of these impacts are diverse across geographies and jurisdictions in which we market, sell and develop our offerings. The depth and duration of the current economic declines attributable to the COVID-19 pandemic, and any potential economic recoveries, are not currently known. In the fourth quarter of fiscal 2020 we experienced revenue declines compared to the fourth quarter of fiscal 2019 and delayed payments from customers. The effect of the pandemic for fiscal 2021 and future periods is unknown. If we are not able to respond to and manage the impact of the COVID-19 pandemic effectively, our business will be harmed." *Oracle Corporation, Annual Report on Form 10-K, filed June 22, 2020 (7372 - Services-Prepackaged Software).*

## *Example 2*

***"Our business may be materially and adversely affected by the ongoing COVID-19 pandemic.***

In December 2019, COVID-19 emerged and has subsequently spread worldwide. The World Health Organization has declared COVID-19 a pandemic resulting in federal, state and local governments and private entities mandating various restrictions, including travel restrictions, restrictions on public gatherings, stay at home orders and advisories and quarantining of people who may have been exposed to the virus. After close monitoring and taking into consideration the guidance from federal, state and local governments, in an effort to mitigate the spread of COVID-19, effective March 19, 2020, the Company closed all of its stores for at least two weeks and has temporarily closed its online businesses, its distribution centers and its offices with Associates working remotely where possible. The Company continues to monitor developments, including government requirements and recommendations at the national, state, and local level to evaluate possible extensions to all or part of such closures.

The temporary closure of our stores, online businesses, distribution centers and offices are expected to have an adverse impact on our results of operations, financial position and liquidity. For example, although our day-to-day operations have been disrupted, we have incurred and may continue to incur labor costs during these closures. In addition, after some or all of our stores re-open, any significant reduction in our customers' willingness to shop our stores, the levels of our customers' spending at our stores or our Associates' willingness to staff our stores and distribution centers, as a result of health concerns related to COVID-19 or its impact on the economy and consumer discretionary spending may impact our business operations, financial performance and liquidity. The extent of the impact of COVID-19 on our business is highly uncertain and difficult to predict, as information is rapidly evolving with respect to the duration and severity of the pandemic and the response to contain it." *The TJX Companies, Inc., Annual Report on Form 10-K filed March 27, 2020 (5651 - Retail-Family Clothing Stores).*

## *Example 3*

***"Changes in U.S., global, and regional economic conditions are expected to have an adverse effect on the profitability of our businesses.***

A decline in economic activity in the U.S. and other regions of the world in which we do business can adversely affect demand for any of our businesses, thus reducing our revenue and earnings. Global economic activity has declined as a result of COVID-19. Past declines in economic conditions reduced spending at our parks and resorts, purchases of and prices for advertising on our broadcast and cable networks and owned stations, performance of our home entertainment releases, and purchases of Company-branded consumer products, and similar impacts can be expected should such conditions recur. The current decline in economic conditions could also reduce attendance at our parks and resorts, prices that MVPDs pay for our cable programming or subscription levels for our cable programming or direct-to-consumer products. Economic conditions can also impair the ability of those with whom we do business to satisfy their obligations to us. In addition, an increase in price levels generally, or in price levels in a particular sector such as the energy sector, could result in a shift in consumer demand away from the entertainment and consumer products we offer, which could also adversely affect our revenues and, at

the same time, increase our costs. A decline in economic conditions could impact implementation of our expansion plans. Changes in exchange rates for foreign currencies may reduce international demand for our products or increase our labor or supply costs in non-U.S. markets, or reduce the U.S. dollar value of revenue we receive and expect to receive from other markets. Economic or political conditions in a country could also reduce our ability to hedge exposure to currency fluctuations in the country or our ability to repatriate revenue from the country." *The Walt Disney Company, Annual Report on Form 10-K filed November 25, 2020 (7990 - Services-Miscellaneous Amusement & Recreation).*

## *Example 4*

***"We experience cybersecurity incidents and might experience significant computer system compromises or data breaches.***

We and our external service providers use sophisticated computer systems to perform our business operations, such as the secure electronic transmission, processing, storage and hosting of sensitive information, including protected health information and other types of personal information, confidential financial information, proprietary information, and other sensitive information relating to our customers, company and workforce. Many of these systems have experienced and are subject to cybersecurity incidents, despite physical, technical and administrative security measures. Cyber incidents include actual or attempted unauthorized access, tampering, malware insertion, ransomware attacks or other system integrity events. The risk of cyber incidents may be increased while many of our personnel are working remotely due to the COVID-19 pandemic. A cybersecurity incident might involve a material data breach or other material impact to the integrity and operations of these computer systems, which might result in litigation or regulatory action, loss of customers or revenue, increased expense, any of which might have a materially adverse impact on our business operations, reputation and our financial position or results of operations." *McKesson Corporation, Annual Report on Form 10-K filed May 22, 2020 (5122 - Wholesale-Drugs Proprietaries & Druggists' Sundries).*

## *Example 5*

***"Changes in technology and in consumer consumption patterns may affect demand for our entertainment products, the revenue we can generate from these products or the cost of producing or distributing products.***

The media entertainment and internet businesses in which we participate increasingly depend on our ability to successfully adapt to shifting patterns of content consumption through the adoption and exploitation of new technologies. New technologies affect the demand for our products, the manner in which our products are distributed to consumers, ways we charge for and receive revenue for our entertainment products and the stability of those revenue streams, the sources and nature of competing content offerings, the time and manner in which consumers acquire and view some of our entertainment products and the options available to advertisers for reaching their desired audiences. This trend has impacted the business model for certain traditional forms of distribution, as evidenced by the industry-wide decline in ratings for broadcast television, the reduction in demand for home entertainment sales of theatrical content, the development of alternative distribution channels for broadcast and cable programming and declines in subscriber levels for traditional cable channels, including for a number of our networks. COVID-19 has accelerated this trend. In order to respond to these developments, we regularly consider, and from time to time implement changes to our business models, most recently by developing, investing in and acquiring DTC products and reorganizing our media and entertainment businesses to accelerate our DTC strategies. There can be no assurance that our DTC offerings and other efforts will successfully respond to these changes. We expect to forgo revenue from traditional sources, particularly as we expand our DTC offerings. There can be no assurance that the DTC model and other business models we may develop will ultimately be as profitable as our existing or historic business models." *The Walt Disney Company, Annual Report on Form 10-K filed November 25, 2020 (7990 - Services-Miscellaneous Amusement & Recreation).*

## *Example 6*

***"Our revenue and results of operations may suffer upon the bankruptcy, insolvency, or other credit failure of a significant customer.***

Most of our customers buy pharmaceuticals and other products and services from us on credit. Credit is made available to customers based upon our assessment and analysis of creditworthiness. Although we often try to obtain a security interest in assets and other arrangements intended to protect our credit exposure, we generally are either subordinated to the position of the primary lenders to our customers or substantially unsecured. Volatility of the capital and credit markets, general economic conditions, and regulatory changes, including changes in reimbursement, may adversely affect the solvency or creditworthiness of our customers. The COVID-19 pandemic has increased volatility of the capital and credit markets and has led to a general worsening of economic conditions, which has

put financial pressure on many of our customers and may threaten certain customers' ability to maintain liquidity sufficient to repay their obligations to us as they become due. The bankruptcy, insolvency, or other credit failure of any customer that has a substantial amount owed to us could have a material adverse effect on our operating revenue and results of operations. As of September 30, 2020, our two largest trade receivable balances due from customers represented approximately 47% and 7% of accounts receivable, net." *AmerisourceBergen Corporation, Annual Report on Form 10-K filed November 19, 2020 (5122 - Wholesale-Drugs Proprietaries & Druggists' Sundries).*

### *Example 7*

***"We are required to maintain the privacy and security of personal and business information amidst evolving threat landscapes and in compliance with emerging privacy and data protection regulations globally. Failure to meet the requirements could damage our reputation with members, suppliers and employees, cause us to incur substantial additional costs, and become subject to litigation.***

Increased IT security threats and more sophisticated computer crime pose a risk to our systems, networks, products and services. We rely upon IT systems and networks, some of which are managed by third parties, in connection with a variety of business activities. Additionally, we collect, store and process sensitive information relating to our business, members, suppliers and employees. Operating these IT systems and networks, and processing and maintaining this data, in a secure manner, is critical to our business operations and strategy. The increased use of remote work infrastructure due to the COVID-19 pandemic has also increased the possible attack surfaces. Security threats designed to gain unauthorized access to our systems, networks and data, are increasing in frequency and sophistication. Cybersecurity attacks may range from random attempts to coordinated and targeted attacks, including sophisticated computer crimes and advanced persistent threats. These threats pose a risk to the security of our systems and networks and the confidentiality, integrity, and availability of our data. It is possible that our IT systems and networks, or those managed by third parties such as cloud providers, could have vulnerabilities, which could go unnoticed for a period of time. While our cybersecurity and compliance posture seeks to mitigate such risks, there can be no guarantee that the actions and controls we and our third-party service providers have implemented and are implementing, will be sufficient to protect our systems, information or other property.

The potential impacts of a future material cybersecurity attack includes reputational damage, litigation, government enforcement actions, penalties, disruption to systems, unauthorized release of confidential or otherwise protected information, corruption of data, diminution in the value of our investment in IT systems and increased cybersecurity protection and remediation costs. This could adversely affect our competitiveness, results of operations and financial condition and loss of member confidence. Further, the amount of insurance coverage we maintain may be inadequate to cover claims or liabilities relating to a cybersecurity attack. In addition, data we collect, store and process is subject to a variety of U.S. and international laws and regulations, such as the European Union's General Data Protection Regulation, California Consumer Privacy Act, Health Insurance Portability and Accountability Act, China cybersecurity law and other emerging privacy and cybersecurity laws across the various states and around the globe, which may carry significant potential penalties for noncompliance." *Costco Wholesale Corporation, Annual Report on Form 10-K filed October 7, 2020 (5331 - Retail-Variety Stores).*

## Risk Factor Disclosure of Brexit-Related Risk

In a 2019 speech, Division of Corporation Finance Director Hinman commented on disclosures of the impact of the United Kingdom's separation from the European Union, commonly known as "Brexit," emphasizing that generic disclosures are not sufficient to "guide investors in a meaningful manner." He stated investors are better served when disclosure provides "tailored insight into how management views the risks posed to the business and operations and what actions they are taking to address these risks," and he provided a non-exhaustive list of topics that companies should consider when developing Brexit-related disclosure. Most companies continue to emphasize that the impact of Brexit remains uncertain. Below are several examples of how companies have disclosed Brexit-related risks.

### *Example 1*

***"The results of the United Kingdom's withdrawal from the EU may have a negative effect on global economic conditions, financial markets and our business.***

We are a multinational company headquartered in the United States with worldwide operations, with significant business operations in Europe, including in the UK. In June 2016, a majority of voters in the UK elected to withdraw from the European Union in a national referendum (Brexit). In March 2017, the government of the UK formally gave notice of its intent to withdraw from the EU. On January 31, 2020, the UK ceased to be a member state of the EU. EU law applicable to the UK continues to apply to and

in the UK for the duration of a transition period which is presently scheduled to expire on December 31, 2020 (the Transition Period). During the Transition Period, the EU and the UK will negotiate the terms of their future relationship. There is no assurance that such negotiations will be successful and it is uncertain what, if any, laws similar to those of the EU will continue to apply in and to the UK following the expiration of the Transition Period. Since a significant proportion of the UK's regulatory framework is derived from EU directives and regulations, EU law ceasing to apply in and to the UK following the expiration of the Transition Period could materially impact the regulatory regime with respect to the movement and approval of our products to and from the UK and EU. We could face new regulatory costs and challenges, a negative impact on the movement of goods and materials in our supply chain, and increased tariffs and duties that could have a material adverse effect on our business, financial condition, cash flows and results of operations. Until expiration of the Transition Period and the future relationship between the EU and the UK is established, it is difficult to anticipate Brexit's potential impact." *Cooper Companies, Inc., Annual Report on Form 10-K filed December 11, 2020 (3851 - Ophthalmic Goods).*

## *Example 2*

***"The United Kingdom's withdrawal from the European Union could harm our business and financial results.***

In June 2016, voters in the United Kingdom approved the withdrawal of the United Kingdom from the European Union (commonly referred to as "Brexit"). In March 2017, the UK government initiated the exit process under Article 50 of the Treaty of the European Union, commencing a period of up to two years for the United Kingdom and the other EU member states to negotiate the terms of the withdrawal, which was subsequently postponed until January 31, 2020, at which point the United Kingdom formally withdrew from the EU. Since then the United Kingdom has continued to participate in the EU from a trade and economic perspective while the parties seek to negotiate a trade deal. The deadline for agreeing to a trade deal is December 31, 2020. Uncertainty over the terms of the United Kingdom's continued participation in the European Union could cause political and economic uncertainty in the United Kingdom and the rest of Europe, which could harm our business and financial results.

Brexit will lead to legal uncertainty and potentially divergent national laws and regulations in the United Kingdom and European Union. We, as well as our clients who have significant operations in the United Kingdom, may incur additional costs and expenses as we adapt to potentially divergent regulatory frameworks from the rest of the European Union and as a result, our Visa operating rules and contractual commitments in the United Kingdom and the rest of the European Union may be impacted. In addition, applications will need to be made for regulatory authorization and permission in separate EU member states following the post-Brexit transition period. These factors may impact our ability to operate and process data in the European Union and United Kingdom seamlessly. This and other Brexit-related issues may require changes to our legal entity structure and/or operations in the United Kingdom and the European Union. Any of these effects of Brexit, among others, could harm our business and financial results." *Visa Inc., Annual Report on Form 10-K filed November 19, 2020 (7389 - Services-Business Services, NEC).*

## *Example 3*

***"Operations and sales outside of the United States may be subject to additional risks.***

A number of risks inherent in international operations could have a material adverse effect on our results of operations, including global health crises, currency fluctuations, difficulties in staffing and managing multi-national operations, general economic and political uncertainties and potential for social unrest in countries in which we operate, limitations on our ability to enforce legal rights and remedies, restrictions on the repatriation of funds, change in trade policies, tariff regulation, difficulties in obtaining export and import licenses and the risk of government financed competition. Issues with the global supply chain can also rise due to some of the aforementioned risks as well as global health crises, such as the COVID-19 pandemic. Furthermore, the Company is subject to laws and regulations, such as the Foreign Corrupt Practices Act, UK Bribery Act and similar local anti-bribery laws, which generally prohibit companies and their employees, agents and contractors from making improper payments for the purpose of obtaining or retaining business. Failure to comply with these laws could subject the Company to civil and criminal penalties that could materially adversely affect the Company's results of operations, financial position and cash flows.

In June 2016, the U.K. held a referendum in which voters approved an exit from the European Union ("E.U.") commonly referred to as "Brexit." The U.K. subsequently withdrew from the European Union on January 31, 2020, subject to a transition period that is set to end on December 31, 2020. Although it is unknown what the terms of the U.K.'s relationship with the E.U. will be, it is possible that there will be greater restrictions on imports and exports between the U.K. and E.U. countries and

increased regulatory complexities. These changes could cause disruptions to and create uncertainty surrounding our business and the business of existing and future customers and suppliers as well as have an impact on our employees based in Europe, which could adversely impact our business. The actual effects of Brexit will depend on any agreements the U.K. makes to retain access to E.U. markets either during a transitional period or more permanently." *TransDigm Group Incorporated, Annual Report on Form 10-K filed November 12, 2020 (3728 – Aircraft Part & Auxiliary Equipment, NEC).*

## *Example 4*

***"We face risks associated with operating in international markets.***

We operate on a global basis, with approximately 42.8% of our net sales coming from operations outside of United States. While geographic diversity helps to reduce the Company's exposure to risks in any one country, we are subject to risks associated with international operations, including, but not limited to:

- political or economic instability or changing macroeconomic conditions in our major markets, including the potential impact of (1) new policies that may be implemented by the U.S. or other jurisdictions, particularly with respect to tax and trade policies or (2) the United Kingdom ("U.K.") voting to leave the European Union ("E.U."), commonly known as Brexit. On March 29, 2017, the U.K. triggered Article 50 of the Lisbon Treaty formally starting a 2 year negotiation period with the E.U., which was subsequently extended to January 31, 2020. The U.K. officially terminated its membership of the E.U. on January 31, 2020 under the terms of a withdrawal agreement concluded between the U.K. and E.U. and is now a transition phase until December 31, 2020. During the transition phase, the U.K. will generally continue operating as if it were still a member of the E.U. Trade talks between the E.U. and U.K., to determine their future relationship, are still underway. If a trade deal is not reached by December 31, 2020, the U.K. can expect checks and tariffs on products going to and coming from the E.U. beginning on January 1, 2021. If a trade deal is not reached by December 31, 2020, the U.K. can expect checks and tariffs on products going to and coming from the E.U. beginning on January 1, 2021. Although the terms of the U.K.'s future relationship with the E.U. are still unknown, it is possible that there will be increased regulatory and legal complexities, including potentially divergent national laws and regulations between the U.K. and E.U. Brexit may also cause disruption and create uncertainty surrounding our business, including affecting our relationships with our existing and future customers, suppliers and employees and resulting in increased cost by way of new or elevated customs duties or financial implications from operational challenges…" *Tapestry, Inc., Annual Report on Form 10-K filed August 13, 2020 (3100 - Leather & Leather Products).*

## *Example 5*

***"The Company conducts operations globally, the risks of which could increase its costs, reduce its profits or disrupt its business.***

. . .

Additionally, in June 2016, voters in the U.K. approved an advisory referendum to withdraw from the E.U., commonly referred to as "Brexit." On January 31, 2020, the U.K. officially terminated its membership in the E.U. pursuant to the terms of a withdrawal agreement concluded between the U.K. and E.U. Among other terms, the withdrawal agreement provides for a transition period through December 31, 2020, during which the U.K.'s existing trade relationship with the E.U. will remain in place and the U.K. will continue to follow the E.U.'s rules. Negotiations during the transition period to determine the U.K.'s future relationship with the E.U., including the terms of a future trade deal, are expected to be complex and it is not clear at this time what, if any, agreements will be reached by the current December 31, 2020 transition period deadline. Changes related to Brexit could significantly disrupt the free movement of goods, services, and people between the U.K. and the E.U., and result in potential higher costs of conducting business in Europe. Brexit could also lead to legal uncertainty and potentially divergent national laws and regulations in the U.K. and the E.U. The Company may incur additional costs and expenses as it adapts to these potentially divergent regulatory frameworks, and may face additional complexity with regard to immigration and travel rights for its employees located in the U.K. and the E.U. There may also be similar referendums or votes in other European countries in which the Company does business. The U.K.'s withdrawal from the E.U. and the uncertainty surrounding the terms of this withdrawal, as well as the impact of any similar circumstances that may arise elsewhere in Europe, could increase the Company's costs and adversely impact consumer and investor confidence.

While these factors, and the effect thereof, are difficult to predict, any one or more of them could lower the Company's revenues, increase its costs, reduce its earnings or disrupt its business." *Tiffany & Co., Annual Report on Form 10-K filed March 20, 2020 (5944 - Retail-Jewelry Stores).*

## Risk Factor Disclosure Related to LIBOR Cessation Risk

In the July 2019 Staff Statement on the LIBOR transition, the Division of Corporation Finance stated that it is important for issuers to keep investors informed about progress toward risk identification and mitigation, as well as on the anticipated impact of the LIBOR transition on the company, if material. The Division of Corporation Finance noted at the time that larger companies and companies in the real estate, insurance and banking industries were most frequently providing LIBOR transition disclosure, but that counterparties from all industries also needed to begin considering the risks and responding to them. The staff statement includes the Division of Corporation Finance's guidance for issuers to consider as they decide what LIBOR-related disclosures are material to their business. Below are several examples of how companies have disclosed risks related to LIBOR cessation.

### *Example 1*

***"We may not effectively manage risks associated with the replacement of benchmark indices.***

The withdrawal and replacement of widely used benchmark indices such as the London Interbank Offered Rate (LIBOR) with alternative benchmark rates may introduce a number of risks for our business, our clients and the financial services industry more widely. These include financial risks arising from potential changes in the valuation of financial instruments linked to benchmark indices, pricing and operational risks, and legal implementation and revised documentation risks. The FCA in the U.K., which regulates LIBOR, has announced that it will no longer compel panel banks to submit rates for LIBOR after 2021. The publication of LIBOR is therefore not guaranteed beyond 2021, and it appears highly likely that LIBOR will be discontinued or modified by the end of 2021. At this time, no consensus exists as to which reference rate or rates or benchmarks may become acceptable alternatives to LIBOR, although the Alternative Reference Rates Committee, a group of market participants convened by the Federal Reserve Board and the Federal Reserve Bank of New York, has identified the Secured Overnight Financing Rate ("SOFR") as the recommend alternative to LIBOR. The selection of SOFR as the alternative reference rate, however, currently presents certain market concerns because a term structure for SOFR has not yet developed, and there is not yet a generally accepted methodology for adjusting SOFR. Accordingly, the withdrawal and replacement of LIBOR may pose financial risks and uncertainties to our business. We also may face operational challenges adopting successor benchmarks." *Franklin Resources, Inc., Annual Report on Form 10-K filed November 23, 2020 (6282 - Investment Advice).*

### *Example 2*

***"LIBOR Indexed Borrowings - The expected phase out of LIBOR could impact the interest rates paid on our variable rate indebtedness and cause our interest expense to increase.***

A substantial portion of our borrowing capacity bears interest at a variable rate based on the London Interbank Offered Rate ("LIBOR"). In July 2017, the United Kingdom's Financial Conduct Authority ("FCA"), which regulates LIBOR, announced that it intends to phase out LIBOR by the end of 2021. The U.S. Federal Reserve, in conjunction with the Alternative Reference Rates Committee, a steering committee comprised of large U.S. financial institutions, is considering replacing LIBOR with the Secured Overnight Financing Rate ("SOFR"), a new index calculated by short-term repurchase agreements, backed by Treasury securities.

Certain of our financing agreements include language to determine a replacement rate for LIBOR, if necessary. However, if LIBOR ceases to exist, we may need to renegotiate some financing agreements extending beyond 2021 that utilize LIBOR as a factor in determining the interest rate. We are evaluating the potential impact of the eventual replacement of the LIBOR benchmark interest rate, however, we are not able to predict whether LIBOR will cease to be available after 2021, whether SOFR will become a widely accepted benchmark in place of LIBOR, or what the impact of such a possible transition to SOFR may be on our business, financial condition, and results of operations." *Amcor plc, Annual Report on Form 10-K filed August 27, 2020 (3990 - Miscellaneous Manufacturing Industries).*

### *Example 3*

***"We may be adversely affected by recent proposals to reform LIBOR.*** Certain of our financial arrangements, including credit facilities, are made at variable interest rates that use the London Interbank Offered Rate, or LIBOR (or metrics derived from or related to LIBOR), as a benchmark for establishing the interest rate. On July 27, 2017, the United Kingdom's Financial Conduct Authority announced that it intends to stop persuading or compelling banks to submit LIBOR rates after 2021. These reforms may cause LIBOR to cease to exist, new methods of calculating LIBOR to be established, or alternative reference rates to be established. The Alternative Reference Rates Committee (ARRC) has proposed that the Secured Overnight Financing Rate (SOFR) is the rate that represents best practice as the alternative to LIBOR for use in financial and other

derivatives contracts that are currently indexed to United States dollar LIBOR. ARRC has proposed a paced market transition plan to SOFR from LIBOR, and organizations are currently working on industry wide and company specific transition plans as it relates to financial and other derivative contracts exposed to LIBOR. Uncertainty exists as to the transition process and broad acceptance of SOFR as the primary alternative to LIBOR, and the potential consequences to us cannot be fully predicted. Changes in market interest rates may influence our financing costs, returns on financial investments and the valuation of derivative contracts and could reduce our earnings and cash flows." *ResMed, Inc., Annual Report on Form 10-K filed August 13, 2020 (3841 - Surgical & Medical Instruments & Apparatus).*

### *Example 4*

***"Our debt instruments impose operating and financial restrictions on us, and in the event of a default, all of our borrowings would become immediately due and payable.***

. . .

In July 2017, the Financial Conduct Authority (the authority that regulates LIBOR) announced it intends to stop compelling banks to submit rates for the calculation of LIBOR after 2021. The Alternative Reference Rates Committee, or ARRC, has proposed that the Secured Overnight Financing Rate, or SOFR, is the rate that represents best practice as the alternative to USD-LIBOR for use in derivatives and other financial contracts that are currently indexed to USD-LIBOR. ARRC has proposed a paced market transition plan to SOFR from USD-LIBOR and organizations are currently working on industry wide and company specific transition plans as it relates to derivatives and cash markets exposed to USD-LIBOR. Establishing a replacement rate for LIBOR in this manner may result in interest obligations which are more than or do not otherwise correlate over time with the payments that would have been made on our debt if LIBOR was available in its current form." *CBRE Group, Inc., Annual Report on Form 10-K filed March 2, 2020 (6500 - Real Estate).*

### *Example 5*

***"The elimination of or change in the London Interbank Offered Rate (LIBOR) may adversely affect the interest rates on and value of certain floating rate securities and other instruments that we hold.***

LIBOR is a common benchmark interest rate (or reference rate) used to set and make adjustments to interest rates for certain floating rate securities and other financial instruments. Published reports have indicated that regulatory authorities and/or financial institutions may change how LIBOR is calculated or discontinue its calculation and publication after 2021. Alternative reference rates have been developed, including The Federal Reserve Bank of New York's Secured Overnight Financing Rate (SOFR), but the acceptance of such alternative rates and their applicability to existing instruments is uncertain. If LIBOR ceases to exist or if the methods of calculating LIBOR change from current methods for any reason, outstanding securities with interest rates tied to LIBOR may be adversely affected if those securities either do not provide for the automatic substitution of another reference rate or convert to another reference rate or a fixed rate that could be less favorable to us. Outstanding securities and contracts that could be affected include certain preferred stocks and other floating rate securities, fixed rate securities that may convert to LIBOR-based floating rate instruments in the future, certain derivatives, and any other assets or liabilities whose value is tied to LIBOR. Any uncertainty regarding the continued use and reliability of LIBOR as a benchmark interest rate could also adversely affect the value of those instruments." *The Progressive Corporation, Annual Report on Form 10-K filed March 2, 2020 (6331 - Fire, Marine & Casualty Insurance).*

### *Example 6*

***"The replacement of LIBOR could adversely affect Truist's profitability and financial condition.***

LIBOR and certain other interest rate benchmarks are the subject of recent national, international and other regulatory guidance and proposals for reform. These reforms may cause such benchmarks to perform differently than in the past or have other consequences which cannot be predicted. The United Kingdom's Financial Conduct Authority, which regulates LIBOR, has publicly announced that it intends to stop compelling banks to submit information to the administrator of LIBOR after 2021. The continuation of LIBOR cannot be guaranteed after 2021. Truist has LIBOR-based contracts that extend beyond 2021 included in loans and leases, securities, deposits, short-term borrowings, long-term debt and derivative financial instruments. While there is no consensus on what rate or rates may become accepted alternatives to LIBOR, a group of market participants convened by the FRB, the ARRC, has selected the SOFR as its recommended alternative to U.S. dollar LIBOR. The FRB of New York started to publish SOFR in April 2018. SOFR is a broad measure of the cost of overnight borrowings collateralized by U.S. Treasury securities.

If SOFR or another alternative reference rate becomes an accepted alternative to LIBOR, it may perform differently

than LIBOR in response to changing market conditions. For example, SOFR could experience greater decreases during times of economic stress, which could require the Company to lend at lower rates at times when the Company's borrowing costs are increasing.

The market transition away from LIBOR to alternative reference rates is complex and could have a range of adverse effects on the Company's business, financial condition and results of operations. In particular, any such transition could:

- adversely affect the interest rates received or paid on the revenue and expenses associated with or the value of the Company's LIBOR-based assets and liabilities;
- adversely affect the interest rates received or paid on the revenue and expenses associated with or the value of other securities or financial arrangements, given LIBOR's role in determining market interest rates globally;
- prompt inquiries or other actions from regulators in respect of the Company's preparation and readiness for the replacement of LIBOR with an alternative reference rate; and
- result in disputes, litigation or other actions with borrowers or counterparties about the interpretation and enforceability of certain fallback language in LIBOR-based contracts and securities.

The transition away from LIBOR to an alternative reference rate will require the transition to or development of appropriate systems, models and analytics to effectively transition the Company's risk management and other processes from LIBOR-based products to those based on the applicable alternative reference rate, such as SOFR. Truist has developed a LIBOR transition team and project plan that outlines timelines and priorities to prepare its processes, systems and people to support this transition. Timelines and priorities include assessing the impact on the Company's clients, as well as assessing system requirements for operational processes. There can be no guarantee that these efforts will successfully mitigate the operational risks associated with the transition away from LIBOR to an alternative reference rate.

The manner and impact of the transition from LIBOR to an alternative reference rate, as well as the effect of these developments on the Company's funding costs, loan, investment and trading securities portfolios, and ALM and business, is uncertain." *Truist Financial Corporation, Annual Report on Form 10-K filed March 3, 2020 (6021 - National Commercial Banks).*

## Risk Factor Disclosure Related to Cybersecurity Risk

Companies continue to have their information technology (IT) systems and networks targeted by malicious third-party actors, and the SEC continues to have a heightened focus on cybersecurity and data privacy risk and risk management disclosure. The SEC adopted cybersecurity interpretive guidance in February 2018. The guidance specifically contemplates when risk factor disclosure is warranted and provides a list of issues for companies to consider when formulating cybersecurity risk factor disclosure. Companies have expanded their disclosures over the past several years in response. This year, companies have added disclosure of the cybersecurity and data privacy risks arising from the rapid shift to remote working as a result of the COVID-19 pandemic, which has left many companies even more vulnerable. Below are several examples of how companies have disclosed cybersecurity and data privacy risk and risk management.

### *Example 1*

***"Cyber security or privacy breaches, or systems and information technology interruption or failure could adversely impact our ability to operate or expose us to significant financial losses and reputational harm.***

We rely heavily on computer, information and communications technology and related systems in order to properly operate our business. From time to time, we experience occasional system interruptions and delays. In the event we are unable to regularly deploy software and hardware, effectively upgrade our systems and network infrastructure and take other steps to maintain or improve the efficiency and efficacy of our systems, the operation of such systems could be interrupted or result in the loss, corruption, or release of data. In addition, our computer and communication systems and operations could be damaged or interrupted by natural disasters, force majeure events, telecommunications failures, power loss, acts of war or terrorism, computer viruses, malicious code, physical or electronic security breaches, intentional or inadvertent user misuse or error or similar events or disruptions. Any of these or other events could cause interruptions, delays, loss of critical and/or sensitive data or similar effects, which could have a material adverse impact on our business, financial condition, protection of intellectual property and results of operations, as well as those of our clients.

In addition, we face the threat to our computer systems of unauthorized access, computer hackers, computer viruses, malicious code, ransomware, phishing, organized cyber-attacks and other security problems and system disruptions,

including possible unauthorized access to and disclosure of our and our clients' proprietary or classified information. In addition, such tactics may also seek to cause payments due to or from the Company to be misdirected to fraudulent accounts, which may not be recoverable by the Company.

While we have security measures and technology in place to protect our and our clients' proprietary or classified information, if these measures fail as a result of a cyber-attack, other third-party action, employee error, malfeasance or otherwise, and someone obtains unauthorized access to our or our clients' information, our reputation could be damaged, our business may suffer and we could incur significant liability. Because the techniques used to obtain unauthorized access or sabotage systems change frequently and generally are not identified until they are launched against a target, we may be unable to anticipate these techniques or to implement adequate preventative measures. As a result, we may be required to expend significant resources to protect against the threat of system disruptions and security breaches or to alleviate problems caused by these disruptions and breaches. Any of these events could damage our reputation and have a material adverse effect on our business, financial condition and results of operations.

In addition, new laws and regulations governing data privacy and the unauthorized disclosure of confidential information, including the European Union General Data Protection Regulation and the California Consumer Privacy Act, pose increasingly complex compliance challenges and potentially elevate costs, and any failure to comply with these laws and regulations could result in significant penalties and legal liability.

We continuously evaluate the need to upgrade and/or replace our systems and network infrastructure to protect our computing environment, to stay current on vendor supported products and to improve the efficiency of our systems and for other business reasons. The implementation of new systems and information technology could adversely impact our operations by imposing substantial capital expenditures, demands on management time and risks of delays or difficulties in transitioning to new systems. In addition, our systems implementations may not result in productivity improvements at the levels anticipated. Systems implementation disruption and any other information technology disruption, if not anticipated and appropriately mitigated, could have an adverse effect on our business." *Jacobs Engineering Group Inc., Annual Report on Form 10-K filed November 24, 2020 (1600 - Heavy Construction Other than Building Const-Contractors).*

### *Example 2*

***"Information technology failures, data security breaches, and the failure to satisfy privacy and data protection laws and regulations could harm our business.***

We use information technology and other computer resources to carry out important operational and marketing activities and to maintain our business records. These information technology systems are dependent upon global communications providers, web browsers, third-party software and data storage providers and other aspects of the Internet infrastructure that have experienced security breaches, cyber-attacks, significant systems failures and service outages in the past. Our normal business activities involve collecting and storing information specific to our homebuyers, employees, vendors and suppliers and maintaining operational and financial information related to our business, both in an office setting and remote locations as needed. A material breach in the security of our information technology systems or other data security controls could include the theft or release of this information. A data security breach, a significant and extended disruption in the functioning of our information technology systems or a breach of any of our data security controls could disrupt our business operations, damage our reputation and cause us to lose customers, adversely impact our sales and revenue and require us to incur significant expense to address and remediate or otherwise resolve these kinds of issues. The unintended or unauthorized disclosure of personal identifying and confidential information as a result of a security breach could also lead to litigation or other proceedings against us by the affected individuals or business partners, or by regulators. The outcome of such proceedings, which could include penalties or fines, could have a significant negative impact on our business.

We may also be required to incur significant costs to protect against damages caused by information technology failures, security breaches, and the failure to satisfy privacy and data protection laws and regulations in the future as legal requirements continue to increase. The European Union and other international regulators, as well as state governments, have recently enacted or enhanced data privacy regulations, such as the California Consumer Privacy Act, and other governments are considering establishing similar or stronger protections. These regulations impose certain obligations for handling specified personal information in our systems, and for apprising individuals of the information we have collected about them. We have incurred costs in an effort to comply with these requirements, and our costs may increase significantly if new requirements are enacted and based on how

individuals exercise their rights. Any noncompliance could result in our incurring substantial penalties and reputational damage, and also could result in litigation.

We provide employee awareness training of cybersecurity threats and routinely utilize information technology security experts to assist us in our evaluations of the effectiveness of the security of our information technology systems, and we regularly enhance our security measures to protect our systems and data. Our increased use of remote work environments and virtual platforms in response to C-19 may also increase our risk of cyber-attack or data security breaches. We use various encryption, tokenization and authentication technologies to mitigate cybersecurity risks and have increased our monitoring capabilities to enhance early detection and rapid response to potential cyber threats. However, because the techniques used to obtain unauthorized access, disable or degrade systems change frequently and often are not recognized until launched against a target, we may be unable to anticipate these techniques or to implement adequate preventative measures. Consequently, we cannot provide assurances that a security breach, cyber-attack, data theft or other significant systems or security failures will not occur in the future, and such occurrences could have a material and adverse effect on our consolidated results of operations or financial position." *D.R. Horton, Inc., Annual Report on Form 10-K filed November 20, 2020 (1531 - Operative Builders).*

## *Example 3*

***"Security vulnerabilities in our IT systems or products as well as unforeseen product errors could have a material adverse impact on our business results of operations, financial condition and reputation***

In the ordinary course of business, we store sensitive data, including intellectual property, personal data, our proprietary business information and that of our customers, suppliers and business partners on our networks. In addition, we store sensitive data through cloud-based services that may be hosted by third parties and in data center infrastructure maintained by third parties. The secure maintenance of this information is critical to our operations and business strategy. Our information systems and those of our partners and customers are subject to the increasing threat of intrusions by a wide range of actors including computer programmers, hackers or sophisticated nation-state and nation-state supported actors or they may be compromised due to employee error or wrongful conduct, malfeasance, or other disruptions. Despite our security measures, and those of our third-party vendors, our information technology and infrastructure has experienced breaches or disruptions and may be vulnerable in the future to breach, attacks or disruptions. If any breach or attack compromises our networks, creates system disruptions or slowdowns or exploits security vulnerabilities of our products, the information stored on our networks or those of our customers could be accessed and modified, publicly disclosed, lost or stolen, and we may be subject to liability to our customers, suppliers, business partners and others, and suffer reputational and financial harm.

In addition, our products are used to manage critical applications and data for customers and third parties may attempt to exploit security vulnerabilities in our products as well as our internal IT systems. As we continue to focus on the development and marketing of security solutions, we become a bigger target for malicious computer hackers, including sophisticated nation-state and nation-state supported actors who wish to exploit security vulnerabilities in our products or IT systems.

We devote significant resources to addressing security vulnerabilities in our IT systems, product solutions and services through our efforts to engineer more secure solutions and services, enhance security and reliability features in our solutions and services, deploy security updates to address security vulnerabilities and seek to respond to known security incidents in sufficient time to minimize any potential adverse impact. Despite our efforts to harden our infrastructure and build secure solutions, from time to time, we experience attacks and other cyber-threats. These attacks can seek to exploit, among other things, known or unknown vulnerabilities in technology included in our IT infrastructure, solutions and services. While we have undertaken efforts to mitigate these vulnerabilities, they could render our internal systems, products, and solutions and services susceptible to a cyber-attack.

Our products may also contain undetected errors or defects when first introduced or as new versions are released. We have experienced these errors or defects in the past in connection with new products and product upgrades. As our products and customer IT infrastructures become increasingly complex, customers may experience unforeseen errors in implementing our products into their IT environments. We expect that these errors or defects will be found from time to time in new or enhanced products after commencement of commercial shipments. These problems may cause us to incur significant warranty and repair costs, divert the attention of our engineering personnel from our product development efforts and cause significant customer relations problems. We may also be subject to liability claims for damages related to product errors or defects. While we carry insurance policies

covering this type of liability, these policies may not provide sufficient protection should a claim be asserted. A material product liability claim may harm our business and results of operations.

Our products must successfully operate with products from other vendors. As a result, when problems occur in a network, it may be difficult to identify the source of the problem. The occurrence of software or hardware problems, whether caused by our products or another vendor's products, may result in the delay or loss of market acceptance of our products. The occurrence of any of these problems may harm our business and results of operations.

Any errors, defects or vulnerabilities in our products or IT systems could result in:

- expenditures of significant financial and product development resources in efforts to analyze, correct, eliminate, or work-around errors and defects or to address and eliminate vulnerabilities;
- remediation costs, such as liability for stolen assets or information, repairs or system damage;
- increased cybersecurity protection costs which may include systems and technology changes, training, and engagement of third party experts and consultants;
- increased insurance premiums;
- loss of existing or potential customers or channel partners;
- loss of proprietary information leading to lost competitive positioning and lost revenues;
- negative publicity and damage to our reputation;
- delayed or lost revenue;
- delay or failure to attain market acceptance;
- an increase in warranty claims compared with our historical experience, or an increased cost of servicing warranty claims, either of which would adversely affect our gross margins; and
- litigation, regulatory inquiries, or investigations that may be costly and harm our reputation." *F5 Networks, Inc., Annual Report on Form 10-K filed November 19, 2020 (3576 - Computer Communications Equipment).*

### *Example 4*

***"We may not be able to prevent, or timely detect, information technology security breaches.***

Security breaches, phishing, spoofing, attempts by others to gain unauthorized access to our information technology systems, networks, and databases and other cyberattacks continue to become more sophisticated and persistent and are sometimes successful. These incidents, which might be related to industrial, state-sponsored, and/or economic espionage, or financial cyber extortion or fraud, include covertly introducing malware and spyware to our computers and networks (or to an electronic system operated by a third party for our benefit) and impersonating authorized users, among others. We seek to detect and investigate all security incidents and to prevent their recurrence, but in some cases, we might be unaware of an incident or its magnitude, duration, and effects. The theft, unauthorized use, transfer, or publication of our intellectual property, our confidential business and/or technical information, or the personal data of our employees and customers by third parties or by our employees could harm our competitive position, reduce the value of our investment in research and development and other strategic initiatives or otherwise adversely affect our business and technology development. To the extent that any security breach or other cybersecurity incident results in inappropriate disclosure of our customers', suppliers', licensees', or employees' confidential information, we may incur liability, face contractual and regulatory fines and penalties, and sustain significant financial resources to remediate such breach. Such an incident could, among other things, also damage our reputation, impair our ability to attract and retain our customers, impact our stock price, and materially damage supplier relationships. If such incident impedes our inability to use or access our information systems for an extended period of time, this could adversely affect our business operations and financial results. In addition, certain suppliers and other third parties with whom we conduct business, including foundries, assembly and test contractors, and distributors, have been, and are likely to continue to be, subject to cybersecurity incidents or network disruptions that could jeopardize our proprietary or sensitive data, impact such third parties' ability to meet their obligations to us, or otherwise negatively impact our ongoing business operations. We expect to continue devoting significant resources to the security of our information technology systems, networks, and databases, including through the training of our employees and monitoring the security posture of critical third parties who have access to our systems or sensitive data. However, we cannot ensure that these security measures and monitoring efforts will be sufficient to prevent or mitigate the damage caused by a cybersecurity incident or network disruption, and our systems may be vulnerable to hacking, insider threats, employee error or manipulation, system malfunctions or other adverse events. While we maintain insurance coverage to mitigate some of these risks, such coverage may be insufficient to cover all losses

or all types of claims that may arise." *Skyworks Solutions, Inc., Annual Report on Form 10-K filed November 17, 2020 (3674 - Semiconductors & Related Devices).*

### *Example 5*

***"Security and/or Data Privacy Breaches, or Disruptions of Our Information Technology Systems Could Adversely Affect Our Business***

The Company relies on information technology networks and systems, including the internet, to process, transmit and store electronic information, and to manage or support a variety of business processes and activities. These technology networks and systems may be susceptible to damage, disruptions or shutdowns due to failures during the process of upgrading or replacing software, databases or components; power outages; telecommunications or system failures; terrorist attacks; natural disasters; employee error or malfeasance; server or cloud provider breaches; and computer viruses or cyberattacks. Cybersecurity threats and incidents can range from uncoordinated individual attempts to gain unauthorized access to information technology networks and systems to more sophisticated and targeted measures, known as advanced persistent threats, directed at the Company, its products, its customers and/or its third-party service providers. Despite the implementation of cybersecurity measures (including access controls, data encryption, vulnerability assessments, continuous monitoring, and maintenance of backup and protective systems), the Company's information technology systems may still be vulnerable to cybersecurity threats and other electronic security breaches. It is possible for such vulnerabilities to remain undetected for an extended period. In addition, it is possible a security breach could result in theft of trade secrets or other intellectual property or disclosure of confidential customer, supplier or employee information. Should the Company be unable to prevent security breaches or other damage to our information technology systems, disruptions could have an adverse effect on our operations, as well as expose the Company to litigation, liability or penalties under privacy laws, increased cybersecurity protection costs, reputational damage and product failure. In addition, we must comply with increasingly complex and rigorous regulatory standards enacted to protect business and personal data in the U.S. and elsewhere. Compliance with privacy and localization laws and regulations increases operational complexity. Failure to comply with these regulatory standards could subject us to fines and penalties, as well as legal and reputational risks, including proceedings against the Company by governmental entities or others." *Emerson Electric Co., Annual Report on Form 10-K filed November 16, 2020 (3600 - Electronic & Other Electrical Equipment (No Computer Equip)).*

### *Example 6*

***"We rely on technology in our business, and any cybersecurity incident, other technology disruption or delay in implementing new technology could negatively affect our business and our relationships with customers.***

We use technology in substantially all aspects of our business operations, and our ability to serve customers most effectively depends on the reliability of our technology systems. We use software and other technology systems, among other things, to generate and select orders, to load and route trucks, to make purchases, to manage our warehouses and to monitor and manage our business on a day-to-day basis. We also use mobile devices, social networking and other online platforms to connect with our employees, suppliers, business partners and customers. Further, our business involves the storage and transmission of numerous classes of sensitive and/or confidential information and intellectual property, including customers' and suppliers' personal information, private information about employees and financial and strategic information about the company and our business partners.

These technology systems and our uses thereof are vulnerable to disruption from circumstances beyond our control, including fire, natural disasters, power outages, systems failures, security breaches, espionage, cyber-attacks, viruses, theft and inadvertent release of information. In particular, we have experienced and continue to experience cybersecurity threats and vulnerabilities in our systems and those of our third party providers, including viruses and attacks targeting our information technology systems and networks.

The ongoing COVID-19 pandemic is introducing additional cybersecurity risk as a result of our employees, contractors and other corporate partners working remotely. Due to the increased remote workforce, we must increasingly rely on information technology systems that are outside our direct control. These systems are potentially vulnerable to cyber-based attacks and security breaches. In addition, cyber criminals are increasing their attacks on individual employees, utilizing interest in pandemic-related information to increase business email compromise scams designed to trick victims into transferring sensitive data or funds, or steal credentials that compromise information systems.

To date, these cybersecurity threats have not had a material impact on our financial condition, results of operations or liquidity. However, the potential consequences of a future

material cybersecurity attack include business disruption; disruption to systems; theft, destruction, loss, corruption, misappropriation or unauthorized release of sensitive and/or confidential information or intellectual property (including personal information in violation of one or more privacy laws); reputational and brand damage; and potential liability, including litigation or other legal actions against us or the imposition by governmental authorities of penalties, fines, fees or liabilities, which, in turn, could cause us to incur significantly increased cybersecurity protection and remediation costs and the loss of customers.

The actions and controls we have implemented and are implementing to date, or which we seek to cause or have caused third party service providers to implement, may be insufficient to protect our systems, information or other intellectual property. Further, we anticipate devoting significant additional resources to upgrade our security measures generally, including those we employ to protect personal information against these cybersecurity threats.

Due to the evolving nature of these cybersecurity threats, the potential impact of any future incident cannot be predicted with certainty, but such an incident could have a material adverse effect on our results of operations and financial condition, especially if the amount of insurance coverage we maintain is not sufficient to cover claims or liabilities relating to the incident.

Further, as we pursue our strategy to grow through acquisitions and to pursue new initiatives that improve our operations and cost structure, we are also expanding and improving our information technologies, resulting in a larger technological presence and corresponding exposure to cybersecurity risk. Failure to adequately assess and identify cybersecurity risks associated with acquisitions and new initiatives would increase our vulnerability to such risks.

Sysco's efforts to prevent security breaches and cybersecurity incidents, and to implement effective disaster recovery plans, may not be entirely effective to insulate us from technology disruption that could result in adverse effects on our results of operations. Additionally, information technology systems continue to evolve and, in order to remain competitive, we must implement new technologies in a timely and efficient manner. If our competitors implement new technologies more quickly or successfully than we do, such competitors may be able to provide lower cost or enhanced services of superior quality compared to those we provide, which could have an adverse effect on our results of operations.

In addition, data privacy is subject to frequently changing rules and regulations, which sometimes conflict among the various jurisdictions and countries where we do business. For example, the EU adopted the GDPR, a new regulation that became effective in May 2018, which requires companies to meet certain requirements regarding the handling of personal data. We are working to comply with GDPR and other laws and regulations in this area that apply to us, such as California's Consumer Privacy Act that became effective January 1, 2020, and we anticipate needing to devote significant additional resources to complying with these laws and regulations. Our failure to successfully implement or comply with appropriate processes to adhere to the requirements of GDPR and other laws and regulations in this area could result in substantial fines or penalties and legal liability and could tarnish our reputation." *Sysco Corporation, Annual Report on Form 10-K filed August 26, 2020 (5140 - Wholesale-Groceries & Related Products).*

### *Example 7*

***"We could be subject to reduced revenues, increased costs, liability claims, or harm to our competitive position as a result of cyberattacks, security vulnerabilities or Internet disruptions.***

We rely upon information technology ("IT") networks, cloud-based platforms, and systems to process, transmit, and store electronic information, and to support a variety of business processes, some of which are provided by third-party vendors. Cyberattacks and security threats are a risk to our business and reputation. A cyberattack, unauthorized intrusion, malicious software infiltration, network disruption or outage, corruption of data, or theft of personal or other sensitive information, could have a material adverse effect on our business operations or that of our clients, result in liability or regulatory sanction, or cause harm to our business and reputation and result in a loss in confidence in our ability to serve clients all of which could have a material adverse effect on our business. The rapid speed of disruptive innovations involving cyberattacks, security vulnerabilities and Internet disruptions enabled by new and emerging technologies may outpace our organization's ability to compete and/or manage the risk appropriately. In addition, cybercriminals may seek to exploit the disruption caused by the COVID-19 pandemic by attempting to engage in payment-related fraud or by more frequently attempting to gain access to our systems through phishing or other means that may be more successful when most of our employees are working remotely.

Data Security and Privacy Leaks: We collect, use, and retain increasingly large amounts of personal information about our clients, employees of our clients, and our employees, including: bank account numbers, credit card numbers,

social security numbers, tax return information, health care information, retirement account information, payroll information, system and network passwords, and other sensitive personal and business information. At the same time, the continued occurrence of high-profile cyber-attacks and data breaches provides evidence of an external environment increasingly hostile to information security. We may be particularly targeted for cyber-attack because of the amount and type of personal and business information that we collect, use, and retain. Vulnerabilities, threats, and more sophisticated and targeted computer crimes pose a risk to the security of our systems and networks, and the confidentiality, availability, and integrity of our data.

Our service platforms enable our clients to store and process personal data on premise or, increasingly, in a cloud-based environment that we host. The security of our IT infrastructure is an important consideration in our customers' purchasing decisions. Because the techniques used to obtain unauthorized access, disable or degrade service or sabotage systems change frequently, are increasingly more complex and sophisticated and may be difficult to detect for long periods of time, we may be unable or fail to anticipate these techniques or implement adequate or timely preventative or responsive measures. As cyber threats continue to evolve, we are focused on ensuring that our operating environments safeguard and protect personal and business information. We may be required to invest significant additional resources to comply with evolving cybersecurity regulations and to modify and enhance our information security and controls, and to investigate and remediate any security vulnerabilities. While we have security systems and IT infrastructure in place designed to detect and protect against unauthorized access to such information, if our security measures are breached, our business could be substantially harmed, and we could incur significant liabilities. Any such breach or unauthorized access could negatively affect our ability to attract new clients, cause existing clients to terminate their agreements with us, result in reputational damage, and subject us to lawsuits, regulatory fines, or other actions or liabilities which could materially and adversely affect our business and operating results. Third-parties, including vendors that provide services for our operations, could also be a source of security risk to us in the event of a failure of their own security systems and infrastructure.

Data Loss and Business Interruption: If our systems are disrupted or fail for any reason, including Internet or systems failure, or if our systems are infiltrated by unauthorized persons, both the Company and our clients could experience data loss, financial loss, harm to reputation, or significant business interruption. Hardware, applications and services, including cloud-based services, that we develop or procure from third-party vendors may contain defects in design or other problems that could compromise the integrity and availability of our services. Any delays or failures caused by network outages, software or hardware failures, or other data processing disruptions, could result in our inability to provide services in a timely fashion or at all. We may be required to incur significant costs to protect against damage caused by disruptions or security breaches in the future. Such events may expose us to unexpected liability, litigation, regulatory investigation and penalties, loss of clients' business, unfavorable impact to business reputation, and there could be a material adverse effect on our business and results of operations." *Paychex, Inc., Annual Report on Form 10-K filed July 17, 2020 (8700 - Services-Engineering, Accounting, Research, Management).*

## Risk Factor Disclosure Related to China-Based Issuers

In November 2020, the Division of Corporation Finance published CF Disclosure Topic No. 10, which provides guidance to companies based in or with the majority of their operations in the People's Republic of China (China-based Issuers). The guidance follows the recommendations of the President's Working Group on Financial Markets and details limitations on the SEC's ability to enforce high-quality disclosure standards for China-based Issuers. Specifically, the guidance warns that investors in China-based Issuers should understand the restrictions on the oversight of accounting firms in connection with audits where audit documents are located in China, restrictions on the U.S.'s ability to investigate and pursue capital markets violations by China-based Issuers, risks associated with investing in variable interest entities and risks arising from the changing legal and regulatory landscape in China. The guidance also provides a list of specific questions for China-based Issuers to consider when developing disclosure about risks to investors. Below are some examples of how companies have disclosed these risks in the past.

### *Example 1*

***"Substantial uncertainties exist with respect to the PRC Foreign Investment Law on how it may impact the viability of our current corporate structure, corporate governance and business operations.***

The PRC Foreign Investment Law, or the FIL, was promulgated on March 15, 2019, and its Implementing Regulation, or the FIL Implementing Regulation, was published on December 31, 2019. The FIL and the FIL Implementing Regulation replaced the Sino-foreign Equity

Joint Venture Enterprise Law, the Sino-foreign Cooperative Joint Venture Enterprise Law and the Wholly Foreign-invested Enterprise Law, together with their implementation rules and ancillary regulations, which herald a new foreign investment regime in China and reflect further opening up to foreign investment. The FIL and the FIL Implementing Regulation embody an expected PRC regulatory trend to rationalize its foreign investment regulatory regime in line with prevailing international practices and legislative efforts to unify corporate legal requirements for both foreign and domestic investments.

Nevertheless, the FIL and the FIL Implementing Regulation are silent on the "variable interest entity" structure, or the VIE structure, and related topics. The VIE structure is adopted by many PRC-based companies, including us, to obtain necessary licenses and permits in industries in China that are currently subject to restrictions or prohibitions on foreign investment and also as a means for domestic companies in China to achieve offshore financing or listing. See "Item 3. Key Information—D. Risk Factors—Risks Related to Our Corporate Structure" and "Item 4. Information on the Company—C. Organizational Structure—Contractual Arrangements with Our Consolidated Affiliated Entities." The FIL removed VIEs from the definition of foreign investment and deleted the definition of "actual control" as a means of identifying foreign investment, which was first mentioned in a 2015 draft of the PRC Foreign Investment Law. However, Article 2 of the FIL states that foreign investment includes the circumstance where foreign investors obtain shares, equity, property shares or other similar rights and interests in enterprises within the territory of China, which leaves space for the PRC government to deal with jurisdiction over VIEs in the future. If the PRC government were to implement restrictions or prohibitions on the VIE structure, our corporate structure and business operations could be negatively impacted." *500.com Limited, Annual Report on Form 20-F filed December 11, 2020 (7990 - Services-Miscellaneous Amusement & Recreation).*

### *Example 2*

***"If additional remedial measures are imposed on the big four PRC-based accounting firms, including our independent registered public accounting firm, in administrative proceedings brought by the SEC alleging the firms' failure to meet specific criteria set by the SEC, with respect to requests for the production of documents, we could be unable to timely file future financial statements in compliance with the requirements of the Exchange Act.***

Beginning in 2011, the Chinese affiliates of the "big four" accounting firms (including our independent registered public accounting firm) were affected by a conflict between the U.S. and Chinese law. Specifically, for certain U.S. listed companies operating and audited in the PRC, the SEC and the PCAOB sought to obtain access to the audit work papers and related documents of the Chinese affiliates of the "big four" accounting firms. The accounting firms were, however, advised and directed that, under Chinese law, they could not respond directly to the requests of the SEC and the PCAOB and that such requests, and similar requests by foreign regulators for access to such papers in the PRC, had to be channeled through the CSRC. In late 2012, this impasse led the SEC to commence administrative proceedings under Rule 102(e) of its Rules of Practice and also under the Sarbanes-Oxley Act of 2002 against the "big four" accounting firms (including our independent registered public accounting firm). A first instance trial of these proceedings in July 2013 in the SEC's internal administrative court resulted in an adverse judgment against the firms. The administrative law judge proposed penalties on the firms, including a temporary suspension of their right to practice before the SEC. Implementation of the latter penalty was postponed pending review by the SEC Commissioners. On February 6, 2015, before a review by the Commissioner had taken place, the firms reached a settlement with the SEC. Under the settlement, the SEC accepts that future requests by the SEC for the production of documents will normally be made to the CSRC. The firms will receive matching Section 106 requests, and are required to abide by a detailed set of procedures with respect to such requests, which in substance require them to facilitate production via the CSRC. If the firms fail to follow these procedures and meet certain other specified criteria, the SEC retains the authority to impose a variety of additional remedial measures, including, as appropriate, an automatic six-month bar on a firm's ability to perform certain audit work, commencement of new proceedings against a firm or, in extreme cases, the resumption of the current administrative proceeding against all four firms.

In the event that the SEC restarts administrative proceedings, depending upon the final outcome, listed companies in the U.S. with major PRC operations may find it difficult or impossible to retain auditors in respect of their operations in the PRC, which could result in their financial statements being determined to not be in compliance with the requirements of the Exchange Act, including possible delisting. Moreover, any negative news about any such future proceedings against the firms may cause investor uncertainty regarding PRC-based, U.S.-listed companies and the market price of their shares may be adversely affected.

If our independent registered public accounting firm was denied, even temporarily, the ability to practice before the SEC and we were unable to timely find another registered

public accounting firm to audit and issue an opinion on our financial statements, our financial statements could be determined not to be in compliance with the requirements of the Exchange Act. Such a determination could ultimately lead to the delisting of our shares from the New York Stock Exchange or deregistration from the SEC, or both, which would substantially reduce or effectively terminate the trading of our shares in the U.S." *Four Seasons Education (Cayman) Inc., Annual Report on Form 20-F filed June 24, 2020 (8200 - Services-Educational Services).*

## *Example 3*

***"Risks Related to Audit Reports Prepared by an Auditor who is not Inspected by the Public Company Accounting Oversight Board***

As a company with shares registered with the U.S. Securities and Exchange Commission, or the SEC, and traded publicly in the United States, our independent registered public accounting firm is required under the laws of the United States to be registered with the Public Company Accounting Oversight Board, or the PCAOB, and undergo regular inspections by the PCAOB to assess its compliance with the laws of the United States and professional standards. The PCAOB, however, is currently unable to inspect a registered public accounting firm's audit work relating to a company's operations in China where the documentation of such audit work is located in China. Accordingly, our independent registered public accounting firm's audit of our operations in China is not subject to the PCAOB inspection. In recent years, the SEC and the PCAOB have issued a number of joint statements highlighting continued challenges faced by the U.S. regulators in their oversight of financial statement audits of U.S.-listed companies with significant operations in China. As part of a continued regulatory focus in the United States on access to audit and other information currently protected by national law, in particular the PRC's, in June 2019, a bipartisan group of lawmakers introduced bills in both houses of the U.S. Congress that would require the SEC to maintain a list of issuers for which PCAOB is not able to inspect or investigate an auditor report issued by a foreign public accounting firm. The Ensuring Quality Information and Transparency for Abroad-Based Listings on our Exchanges (EQUITABLE) Act prescribes increased disclosure requirements for these issuers and, beginning in 2025, the delisting from U.S. national securities exchanges such as the New York Stock Exchange of issuers included on the SEC's list for three consecutive years. Enactment of this legislation or other efforts to increase U.S. regulatory access to audit information could cause investor uncertainty for affected issuers, including us, and the market price of our ADSs could be adversely affected. It is unclear if this proposed legislation would be enacted.

The PCAOB has conducted inspections of independent registered public accounting firms outside of China and has at times identified deficiencies in the audit procedures and quality control procedures of those accounting firms. Such deficiencies may be addressed in those accounting firms' future inspection process to improve their audit quality. Due to the lack of PCAOB inspections of audit work undertaken in China, our investors do not have the benefit of the PCAOB inspection of our independent registered public accounting firm's audit work and audit quality control procedures." *PetroChina Company Limited, Annual Report on Form 20-F filed April 29, 2020 (1311 - Crude Petroleum & Natural Gas).*

**Christina Thomas, Partner, Mayer Brown LLP**

Christina Thomas is a partner in Mayer Brown's Washington DC and New York offices and a member of the Capital Markets practice. Christina represents US and foreign companies, investment banks and sponsors on securities offerings, mergers and acquisitions, US Securities and Exchange Commission (SEC) disclosure requirements, shareholder proposals, and ESG matters.

Christina is a former senior advisor at the SEC, serving most recently as Counsel to SEC Commissioner Elad L. Roisman. In that role, she provided legal counsel to the Commissioner on his consideration of policy, regulatory, and enforcement matters.

She advised on SEC proposed and final rule amendments, interpretations, and guidance relating to, among other things, public company disclosure, the proxy voting process, and capital formation. Christina advised on major rulemakings, including modernization of Regulation S-K disclosure requirements, the update of statistical disclosures

for bank and savings and loan registrants, amendments to financial disclosure requirements for acquired and disposed businesses, exemptions from the proxy rules for proxy voting advice, amendments to the shareholder proposal rule, extension of the "test-the-waters" accommodation to all issuers, amendments to the "accredited investor" definition, and harmonization of the exempt offering framework.

She also served as lead advisor on international securities law and policy. Prior to serving as counsel to the Commissioner, Christina was detailed to the US Department of the Treasury to advise on international securities law matters. She received the Secretary's Honor Award in recognition of her contributions. Christina began her career at the SEC in its Division of Corporation Finance in the Office of Healthcare and Insurance (now Life Sciences). She also served as a reviewer on the SEC's Shareholder Proposal Task Force and in the Office of Mergers and Acquisitions.