Market Trends 2020/21: Cybersecurity-Related Disclosures

A Practical Guidance® Practice Note by Anna T. Pinedo, Gonzalo D.V. Go III, Nicole Cors, and Felix R. Zhang, Mayer Brown LLP

Anna T. Pinedo
Mayer Brown LLP

Gonzalo D.V. Go III
Mayer Brown LLP

Nicole Cors,
Mayer Brown LLP

This practice note identifies cybersecurity risk disclosures that offer detailed discussions on the potential reputational, financial, or operational harm resulting from cybersecurity breaches as well as the potential litigation or regulatory costs, policies, and procedures in addressing cybersecurity risks. This practice note concludes with practical advice on how to prepare and enhance the required disclosures on cybersecurity risks and incidents.

SEC Focus

The Securities and Exchange Commission (SEC) has been focused on cybersecurity issues for over a decade, tracing back to its initial guidance on this topic in 2011. On October 16, 2018, the SEC released a report pursuant to Section 21(a) (15 U.S.C. § 78u) of the Securities Exchange Act of 1934, as amended (the Exchange Act) detailing its investigation of several public companies that were victims of cybersecurity-related frauds. See Release No. 84429, available here. While the SEC decided not to pursue enforcement actions against these companies, it emphasized the duty of a public company to comply with the requirements of Section 13(b)(2)(B) (15 U.S.C. § 78m) of the Exchange Act to devise and maintain a sufficient system of internal accounting controls.

On December 6, 2018, former SEC Chairman Jay Clayton, in a speech, highlighted cybersecurity risks as one of the prominent challenges the SEC faces. Former Chairman Clayton reiterated the SEC's statement and interpretive guidance regarding disclosures on cybersecurity risks and incidents issued earlier in 2018 (2018 Guidance).

Under the 2018 Guidance, public companies are required to disclose cybersecurity risks and cyber incidents to the extent that these are material. In evaluating whether cybersecurity risks or incidents are material, a public company should consider, among other things, the nature and magnitude of cybersecurity risks or prior incidents; the actual or potential harms of a cyber breach to the company's reputation, financial condition, or business operation; the legal and regulatory requirements to

which the company is subject; the costs associated with cybersecurity protection, including preventive measures and insurance; and the costs associated with cybersecurity incidents, including remedial measures, investigations, responding to regulatory actions, and addressing litigation.

Once cybersecurity risks and incidents are determined to be material, a public company should provide complete and accurate information in its periodic reports regarding these risks, incidents, and related investigations or litigation.

Public companies generally include cybersecurity-related disclosures in the following sections of their offering materials and periodic reports: Risk Factors, Business, and Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A). Most of the initial cybersecurity disclosures were generic boilerplate provisions or laundry lists of risks applicable to almost any company. These disclosures simply included general statements about cybersecurity risks and incidents but did not particularly disclose how cybersecurity risks and incidents might impact the company, its management, operations, and prospects. At present, companies commonly provide detailed discussions of ongoing cybersecurity litigations and actions in their notes to financial statements that are incorporated by reference in offering materials or periodic reports. This practice note identifies some cybersecurity-related disclosures that offer more detailed discussions of effects.

For further information on public company disclosure in general, see Top 10 Practice Tips: Periodic and Current Public Company Reporting, Public Company Periodic Reporting and Disclosure Obligations, and Periodic and Current Reporting Resource Kit.

Other SEC Activity on Cybersecurity

On January 27, 2020, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a report of observations arising from OCIE's examinations on how various broker-dealers, investment advisers, clearing agencies, national securities exchanges, and other SEC registrants manage cybersecurity risks and enhance operational resiliency. The report is available at this link. OCIE classified its cybersecurity practices into seven categories: governance and risk management, access rights and controls, data loss prevention, mobile security, incident response and resiliency, vendor management, and training and awareness.

On July 10, 2020, the SEC issued a risk alert on ransomware. See Cybersecurity: Ransomware Alert, available at this link. Ransomware is a type of malware which infiltrates a company's electronic systems and denies the company access until it pays a ransom. The alert identified techniques used by such hackers and mitigation strategies that companies may take (including, among others, training and awareness of the threat).

Cybersecurity Disclosures in the Risk Factors Section

Item 105 (17 C.F.R. § 229.105) of Regulation S-K requires a description of material risks that impact a business; how these risks affect the issuer's financial position, results of operations, and future prospects; and how an investment in the offered securities becomes speculative or riskier because of these risks. For further information, see Market Trends 2020/21: Risk Factors, Top 10 Practice Tips: Risk Factors, and Risk Factor Drafting for a Registration Statement. The disclosures should be in plain English and should not be generic. For further information on plain English, see Top 10 Practice Tips: Drafting a Registration Statement and Glossaries in Prospectuses and Annual Reports—Background.

A majority of companies choose to disclose cybersecurity risks in the Risk Factors section. The nature of the disclosures varies by company, but companies that have a strong e-commerce presence or that have experienced a security breach typically provide disclosure with particularity. Companies that are subject to industry regulations on cybersecurity, such as financial services companies, may want to enhance their disclosures by discussing the relevant regulatory developments on cybersecurity. When a cybersecurity breach occurs, a company typically discloses such incident, together with the remedial actions the company is planning to undertake, estimated losses arising from the breach, and whether there are litigation and regulatory actions or other consequences associated with the cybersecurity breach. For a further discussion on cybersecurity disclosure, see Media & Entertainment Industry Guide for Capital Markets. Set forth below are some examples of cybersecurity disclosures in the Risk Factors section.

General Disclosure on Cybersecurity Risks

- **"TEC is exposed to potential risks related to cyberattacks and unauthorized access, which could cause system failures, disrupt operations or adversely affect safety.**

  TEC increasingly relies on information technology systems and network infrastructure to manage its business and safely operate its assets, including controls

for interconnected systems of generation, distribution and transmission and financial, billing and other business systems. TEC also relies on third party service providers to conduct business. As TEC operates critical infrastructure, it may be at greater risk of cyberattacks by third parties, which could include nation-state controlled parties.

Cyberattacks can reach TEC's networks with access to critical assets and information via their interfaces with less critical internal networks or via the public internet. Cyberattacks can also occur via personnel with direct access to critical assets or trusted networks. An outbreak of infectious disease, a pandemic or a similar public health threat, such as COVID-19, may cause disruption in normal working patterns including wide scale 'work from home' policies, which could increase cybersecurity risk as the quantity of both cyberattacks and network interfaces increases. . . . Methods used to attack critical assets could include general purpose or energy-sector-specific malware delivered via network transfer, removable media, viruses, attachments or links in e-mails. The methods used by attackers are continuously evolving and can be difficult to predict and detect.

TEC's systems, assets and information could experience security breaches that could cause system failures, disrupt operations or adversely affect safety. Such breaches could compromise customer, employee-related or other information systems and could result in loss of service to customers or the unavailability, release, destruction or misuse of critical, sensitive or confidential information. These breaches could also delay delivery or result in contamination or degradation of hydrocarbon products TEC transports, stores or distributes.

Should such cyberattacks or unauthorized accesses materialize, TEC could suffer costs, losses and damages all, or some of which, may not be recoverable through insurance, legal, regulatory cost recovery or other processes. If not recovered through these means, they could materially adversely affect TEC's business and financial results including its reputation and standing with customers, regulators, governments and financial markets. Resulting costs could include, amongst others, response, recovery and remediation costs, increased protection or insurance costs and costs arising from damages and losses incurred by third parties. If any such security breaches occur, there is no assurance that they can be adequately addressed in a timely manner.

With respect to certain of its assets, TEC is required to comply with rules and standards relating to cybersecurity and information technology including, but not limited to, those mandated by bodies such as the North American Electric Reliability Corporation. TEC cannot be assured that its operations will not be negatively impacted by a cyberattack." *Tampa Electric Company, Form 10-K filed on February 16, 2021 (SIC 4911—Electric Services).*

- **"Our business could be negatively affected by security threats.**

  A cyberattack or similar incident could occur and result in information theft, data corruption, operational disruption, damage to our reputation or financial loss. Our industry has become increasingly dependent on digital technologies to conduct certain exploration, development, production, processing and financial activities. Our technologies, systems, networks, or other proprietary information, and those of our vendors, suppliers and other business partners, may become the target of cyberattacks or information security breaches that could result in the unauthorized release, gathering, monitoring, misuse, loss or destruction of proprietary and other information, or could otherwise lead to the disruption of our business operations. Cyberattacks are becoming more sophisticated and certain cyber incidents, such as surveillance, may remain undetected for an extended period and could lead to disruptions in critical systems or the unauthorized release of confidential or otherwise protected information. These events could lead to financial loss from remedial actions, loss of business, disruption of operations, damage to our reputation or potential liability. Also, computers control nearly all the oil and gas distribution systems in the United States and abroad, which are necessary to transport our production to market. A cyberattack directed at oil and gas distribution systems could damage critical distribution and storage assets or the environment, delay or prevent delivery of production to markets and make it difficult or impossible to accurately account for production and settle transactions. Cyber incidents have increased, and the United States government has issued warnings indicating that energy assets may be specific targets of cybersecurity threats. Our systems and insurance coverage for protecting against cybersecurity risks may not be sufficient. Further, as cyberattacks continue to evolve, we may be required to expend significant additional resources to continue to modify or enhance our protective measures or to investigate and remediate any vulnerability to cyberattacks." *Blue Dolphin Energy Company, Form 10-K filed on March 30, 2021 (SIC 1311—Crude Petroleum & Natural Gas).*

- **"Our information technology systems and the information technology systems of third parties with whom we do business are vulnerable to cyber-attacks, breaches of security and misappropriation of**

data, which could result in substantial damage to our business and operations.

Our internal computer systems and those of our current and future employees and third-party vendors, manufacturers, licensees and consultants are vulnerable to damage from unauthorized access, natural disasters, terrorism, war and telecommunication and electrical failures. The secure processing, maintenance and transmission of electronic information, including customer, employee and company data, is critical to our operations and the legal environment surrounding information security, storage, use, processing, disclosure and privacy is demanding with the frequent imposition of new and changing requirements. We also store certain information with third parties, and we utilize third-party service providers to process, manage or transmit data, which may also increase our risk. Our information systems and those of third parties with whom we do business are subjected to computer viruses or other malicious codes, cyber- or phishing-attacks and also are vulnerable to an increasing threat of continually evolving cybersecurity risks and external hazards, as well as improper or inadvertent employee behavior, all of which could expose confidential company and personal data systems and information to security breaches. Any system failure or security breach by employees or others may pose a risk that sensitive data, including data from our target animal studies, intellectual property, trade secrets, confidential information or personal information belonging to us may be exposed to unauthorized persons or to the public. If such an event were to occur and cause interruptions in our operations, it could result in a material disruption of our development programs and our business operations. For example, the loss of data from completed or future studies could result in delays in our regulatory approval efforts and significantly increase our costs to recover or reproduce the data. Likewise, we rely on third parties to manufacture our therapeutics and therapeutic candidates, and similar events relating to their computer systems could also have a material adverse effect on our business. To the extent that any disruption or security breach were to result in a loss of, or damage to, our data or applications, or inappropriate disclosure of confidential or proprietary information, we could incur liability, the further development of our therapeutic candidates and commercialization of our therapeutics could be delayed, and the trading price of our common stock could be adversely affected. To date, we have not experienced any material impact to our business or operations resulting from security breaches, including from information or cybersecurity attacks; however, because of the frequently changing attack techniques, along with the increased volume and sophistication of the attacks, there is the potential for us to be adversely impacted." *Kindred Biosciences, Inc., Form 10-K filed on March 16, 2021 (SIC 2834—Pharmaceutical Preparations).*

- **"System failure or cybersecurity breaches of our network security could subject us to increased operating costs as well as litigation and other potential losses.**

  We rely heavily on communications and information systems to conduct our business. The computer systems and network infrastructure we use could be vulnerable to unforeseen hardware and cybersecurity issues. Our operations are dependent upon our ability to protect our computer equipment against damage from fire, power loss, telecommunications failure or a similar catastrophic event. Any damage or failure that causes an interruption in our operations could have an adverse effect on our financial condition and results of operations. In addition, our operations are dependent upon our ability to protect the computer systems and network infrastructure we use, including our Internet banking activities, against damage from physical break-ins, cybersecurity breaches and other disruptive problems caused by the internet or users. Such problems could jeopardize the security of our customers' personal information and other information stored in and transmitted through our computer systems and network infrastructure, which may result in significant liability to us, subject us to additional regulatory scrutiny, damage our reputation, result in a loss of customers or inhibit current and potential customers from our internet banking services. Any or all of these problems could have a material adverse effect on our results of operations and financial condition. Although we have security measures, including firewalls and penetration tests, designed to mitigate the possibility of break-ins, breaches and other disruptive problems, there can be no assurance that such security measures will be effective in preventing such problems.

  We are dependent on our information technology and telecommunications systems and third-party service providers; systems failures, interruptions and cybersecurity breaches could have a material adverse effect on us.

  Our business is dependent on the successful and uninterrupted functioning of our information technology and telecommunications systems and third-party service providers. The failure of these systems, or the termination of a third-party software license or service agreement on which any of these systems is based, could interrupt our operations. Because our information technology and telecommunications systems

interface with and depend on third-party systems, we could experience service denials if demand for such services exceeds capacity or such third-party systems fail or experience interruptions. If significant, sustained or repeated, a system failure or service denial could compromise our ability to operate effectively, damage our reputation, result in a loss of customer business and/or subject us to additional regulatory scrutiny and possible financial liability, any of which could have a material adverse effect on us.

Our third-party service providers may be vulnerable to unauthorized access, computer viruses, phishing schemes and other security breaches. We likely will expend additional resources to protect against the threat of such security breaches and computer viruses, or to alleviate problems caused by such security breaches or viruses. To the extent that the activities of our third-party service providers or the activities of our customers involve the storage and transmission of confidential information, security breaches and viruses could expose us to claims, regulatory scrutiny, litigation costs and other possible liabilities.

The occurrence of fraudulent activity, breaches or failures of our information security controls or cybersecurity-related incidents could have a material adverse effect on our business, financial condition, results of operations and growth prospects.

As a bank, we are susceptible to fraudulent activity, information security breaches and cybersecurity-related incidents that may be committed against us or our customers, which may result in financial losses or increased costs to us or our customers, disclosure or misuse of our information or our customer information, misappropriation of assets, privacy breaches against our customers, litigation or damage to our reputation. Such fraudulent activity may take many forms, including check fraud, electronic fraud, wire fraud, phishing, social engineering and other dishonest acts. Information security breaches and cybersecurity-related incidents may include fraudulent or unauthorized access to systems used by us or our customers, denial or degradation of service attacks and malware or other cyber-attacks. In recent periods, there continues to be a rise in electronic fraudulent activity, security breaches and cyber-attacks within the financial services industry, especially in the commercial banking sector due to cyber criminals targeting commercial bank accounts. Moreover, in recent periods, several large corporations, including financial institutions and retail companies, have suffered major data breaches, in some cases exposing not only confidential and proprietary corporate information, but also sensitive financial and other personal information of their customers and employees and subjecting them to potential fraudulent activity. Some of our customers may have been affected by these breaches, which could increase their risks of identity theft and other fraudulent activity that could involve their accounts with us.

Information pertaining to us and our customers is maintained, and transactions are executed, on networks and systems maintained by us and certain third-party partners, such as our online banking, mobile banking or accounting systems. The secure maintenance and transmission of confidential information, as well as execution of transactions over these systems, are essential to protect us and our customers against fraud and security breaches and to maintain the confidence of our customers. Breaches of information security also may occur through intentional or unintentional acts by those having access to our systems or the confidential information of our customers, including employees. In addition, increases in criminal activity levels and sophistication, advances in computer capabilities, new discoveries, vulnerabilities in third-party technologies (including browsers and operating systems) or other developments could result in a compromise or breach of the technology, processes and controls that we use to prevent fraudulent transactions and protect data about us, our customers and underlying transactions, as well as the technology used by our customers to access our systems. Our third-party partners' inability to anticipate, or failure to adequately mitigate, breaches of security could result in a number of negative events, including losses to us or our customers, loss of business or customers, damage to our reputation, the incurrence of additional expenses, disruption to our business, additional regulatory scrutiny, penalties or exposure to civil litigation and possible financial liability, any of which could have a material adverse effect on our business, financial condition, results of operations and growth prospects." *Home Bancorp, Inc., Form 10-K filed on March 9, 2021 (SIC 6036— Savings Institutions, Not Federally Chartered).*

Disclosure for Companies That Have a Strong E-commerce Presence

- **"Failure to protect the integrity and security of individually identifiable data of our customers and employees could expose us to litigation and damage our reputation; the expansion of our e-commerce business has inherent cybersecurity risks that may result in business disruptions.**

  We receive and maintain certain personal information about our customers and employees in the ordinary course of business. Our use of this information is

regulated at the international, federal and state levels, as well as by certain third parties with whom we contract for such services. If our security and information systems are compromised or our business associates fail to comply with these laws and regulations and this information is obtained by unauthorized persons or used inappropriately, it could adversely affect our reputation, as well as operations, results of operations, and financial condition and could result in litigation or the imposition of penalties. As privacy and information security laws and regulations change, we may incur additional costs to ensure we remain in compliance. Our business requires collection of large volumes of internal and customer data, including credit card numbers and other personally identifiable information of our customers in various information systems and those of our service providers. The integrity and protection of customer, employee, and company data is critical to us. If that data is inaccurate or incomplete, we or the store employees could make faulty decisions. Customers and employees also have a high expectation that we and our service providers will adequately protect their personal information. The regulatory environment surrounding information, security and privacy is also increasingly demanding. Our existing systems may be unable to satisfy changing regulatory requirements and employee and customer expectations, or may require significant additional investments or time to do so. Despite implementation of various measures designed to protect our information systems and records, including those we maintain with our service providers, we may be subject to security breaches, system failures, viruses, operator error or inadvertent releases of data. A significant theft, loss, or fraudulent use of customer, employee, or company data maintained by us or by a service provider or failure to comply with the various United States and international laws and regulations applicable to the protection of such data or with Payment Card Industry data security standards, could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. A breach in the security of our information systems or those of our service providers could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.

Certain aspects of the business, particularly our website, heavily depend on consumers entrusting personal financial information to be transmitted securely over public networks. We have experienced increasing e-commerce sales over the past several years, which increases our exposure to cybersecurity risks. We invest considerable resources in protecting the personal information of our customers but are still subject to the risks of security breaches and cyber incidents resulting in unauthorized access to stored personal information. Any breach of our cybersecurity measures could result in violation of privacy laws, potential litigation, and a loss of confidence in our security measures, all of which could have a negative impact on our financial results and our reputation. In addition, a privacy breach or other type of cybercrime or cybersecurity attack could cause us to incur significant costs to restore the integrity of our system, could require the devotion of significant management resources, and could result in significant costs in government penalties and private litigation." *Kirkland's Inc., Form 10-K filed on March 26, 2021 (SIC 5990—Retail—Retail Stores, NEC).*

- **"Failure to protect our website, networks and computer systems against disruption and cyber security threats, or otherwise protect our and our customers' confidential information, could damage our relationships with our customers, harm our reputation, expose us to litigation and adversely affect our business.**

  We rely extensively on our computer systems for the successful operation of our business, including corporate email communications to and from employees, customers and retail operations, the design, manufacture and distribution of our finished goods, digital marketing efforts, collection and retention of customer data, employee information, the processing of credit card transactions, online e-commerce activities and our interaction with the public in the social media space. Our systems are subject to damage or interruption from computer viruses, malicious attacks and other security breaches. The possibility of a cyber-attack on any one or all of these systems is always a serious threat and consumer awareness and sensitivity to privacy breaches and cyber security threats is at an all-time high. If a cybersecurity incident occurs, or there is a public perception that we have suffered a breach, our reputation and brand could be damaged and we could be required to expend significant capital and other resources to alleviate problems.

  As part of our business model, we collect, retain, and transmit confidential information over public networks. In addition to our own databases, we use third party service providers to store, process and transmit this information on our behalf. Although we contractually require these service providers to implement and use reasonable security measures, we cannot control third parties and cannot guarantee that a security breach will not occur in the future either at their location or within their systems. We have confidential security measures in place to protect both our physical facilities and digital

systems from attacks. Despite these efforts, we may be vulnerable to targeted or random security breaches, acts of vandalism, computer viruses, misplaced or lost data, programming and/or human errors, or other similar events.

Given the robust nature of our e-commerce presence and digital strategy, it is imperative that we and our e-commerce partners maintain uninterrupted operation of our: (i) computer hardware, (ii) software systems, (iii) customer marketing databases, and (iv) ability to email our current and potential customers.

If our systems are damaged or fail to function properly or reliably, we may incur substantial repair or replacement costs, experience data loss or theft and impediments to our ability to conduct our operations. Any material disruptions in our e-commerce presence or information technology systems could have a material adverse effect on our business, financial condition and results of operations." *1-800-FLOWERS.COM, Inc., Form 10-K filed on September 11, 2020 (SIC 5990 Retail—Retail Stores—NEC).*

Disclosures on Intersection of Cybersecurity and Data Privacy

- **"We rely heavily on information technology, and any material failure, weakness, interruption or breach of security could prevent us from effectively operating our business.**

  We rely heavily on information systems, including point-of-sale processing in our restaurants, for management of our supply chain, inventory, payment of obligations, collection of cash, credit and debit card transactions, training, human capital management, financial tools and other business processes and procedures. Our ability to efficiently and effectively manage our business functions depends significantly on the reliability and capacity of these systems. Our operations depend upon our ability to protect our computer equipment and systems against damage from physical theft, fire, power loss and outages, telecommunications failure or other catastrophic events, as well as from internal and external security breaches, viruses and other disruptive problems. The failure of these systems to operate effectively, whether from maintenance problems, upgrading or transitioning to new platforms, or a breach in security of these systems, could result in interruptions or delays in our restaurant or other operations, adversely impacting the restaurant experience for our guests and reduce efficiency or negatively impacting our operations. If our information technology systems fail and our redundant systems or disaster recovery plans are not adequate to address such failures, or if our business interruption insurance does not sufficiently compensate us for any losses that we may incur, our revenues and profits could be reduced and the reputation of our brand and our business could be materially adversely affected. In addition, remediation of any problems with our systems could result in significant, unplanned expenses. We have instituted controls, including information system governance controls that are intended to protect our computer systems, our point of sale (POS) systems, and our information technology systems and networks; and adhere to payment card industry data security standards and limit third party access for vendors that require access to our restaurant networks. We also have business continuity plans that attempt to anticipate and mitigate failures. However, we cannot control or prevent every potential technology failure, adverse environmental event, third-party service interruption or cybersecurity risk.

  We collect and maintain personal information about our employees and our guests and are seeking to provide our guests with new digital experiences. These digital experiences may require us to open up access into our Point of Sale systems to allow for capabilities like mobile order and pay and third party delivery. The collection and use of personal information is regulated at the federal and state levels; such regulations include the California Consumer Privacy Act (CCPA) effective January 1, 2020 and which will require our instituting new processes and protections. The CCPA provides a new private right of action and requires companies that process information on California residents to make new disclosures to consumers about their data collection, use and sharing practices and allow consumers to opt out of certain data sharing with third parties. If we fail to properly respond to security breaches of our or third party's information technology systems or fail to properly respond to consumer requests under the CCPA, we could experience reputational damage, adverse publicity, loss of consumer confidence, and regulatory and legal risk, including criminal penalties or civil liabilities.

  We increasingly rely on cloud computing and other technologies that result in third parties holding significant amounts of customer or employee information on our behalf. There has been an increase over the past several years in the frequency and sophistication of attempts to compromise the security of these types of systems. If the security and information systems that we or our outsourced third-party providers use to store or process such information are compromised or if we, or such third parties, otherwise fail to comply with applicable laws and regulations, we could face litigation and the imposition of penalties that could adversely affect our

financial performance. Our reputation as a brand or as an employer could also be adversely affected by these types of security breaches or regulatory violations, which could impair our ability to attract and retain qualified employees." *Del Taco Restaurants, Inc., Form 10-K filed on March 11, 2021 (SIC 5812—Retail—Eating Places).*

- **"We rely significantly on information technology systems and any failure, inadequacy, interruption or security lapse of that technology, including any cybersecurity incidents, could harm our ability to operate our business effectively and have a material adverse effect on our business, reputation, financial condition, and results of operations.**

  [. . .] As part of our business, we collect, store and transmit large amounts of confidential information, proprietary data, intellectual property and personal data. The information and data processed and stored in our technology systems, and those of our research collaborators, CROs, contract manufacturers, suppliers, distributors, or other third parties for which we depend to operate our business, may be vulnerable to loss, damage, denial-of-service, unauthorized access or misappropriation. Data security breaches may be the result of unauthorized or unintended activity (or lack of activity) by our employees or contractors or malware, hacking, business email compromise, phishing or other cyberattacks directed by third parties. These third parties for which we depend on to operate our business have experienced and may continue to experience cybersecurity incidents. While we have implemented measures to protect our information and data stored in our technology systems and those of the third parties that we rely on, our efforts may not be successful.

  We have experienced and may continue to experience cybersecurity incidents. Although to our knowledge we have not experienced any material incident or interruption to date, if such an event were to occur it could result in a material disruption of our development programs and commercial operations, including due to a loss, corruption or unauthorized disclosure of our trade secrets, personal data or other proprietary or sensitive information. Further, these cybersecurity incidents can lead to the public disclosure of personal information (including sensitive personal information) of our employees, clinical trial patients and others and result in demands for ransom or other forms of blackmail. Such attacks are of ever-increasing levels of sophistication and are made by groups and individuals with a wide range of motives (including industrial espionage) and expertise, including by organized criminal groups, 'hacktivists,' nation states and others. Moreover, the costs to us to investigate and mitigate cybersecurity incidents could be significant. For example, the loss of clinical trial data could result in delays in our product development or regulatory approval efforts and significantly increase our costs to recover or reproduce the data. Any security breach that results in the unauthorized access, use or disclosure of personal data may require us to notify individuals, governmental authorities, credit reporting agencies, or other parties pursuant to privacy and security laws and regulations or other obligations. Such a security compromise could harm our reputation, erode confidence in our information security measures, and lead to regulatory scrutiny. To the extent that any disruption or security breach resulted in a loss of, or damage to, our data or systems, or inappropriate disclosure of confidential, proprietary or personal information, we could be exposed to a risk of loss, enforcement measures, penalties, fines, indemnification claims, litigation and potential civil or criminal liability, which could materially adversely affect our business, financial condition and results of operations." *BioMarin Pharmaceutical Inc., Form 10-K filed on February 26, 2021 (SIC 2834—Pharmaceutical Preparations).*

Disclosures Relating to Actual or Known Cybersecurity Breaches and Remedial Measures

- **"If our efforts to provide information security, cybersecurity, and data privacy are unsuccessful or if we are unable to meet increasingly demanding regulatory requirements, we may face additional costly government enforcement actions and private litigation, and our reputation and results of operations could suffer.**

  [. . .] Prior to 2013, all data security incidents we encountered were insignificant. Our 2013 data breach was significant and went undetected for several weeks. Both we and our vendors have had data security incidents since the 2013 data breach; however, to date these other incidents have not been material to our results of operations. Based on the prominence and notoriety of the 2013 data breach, even minor additional data security incidents could draw greater scrutiny. If we, our vendors, or other third parties with whom we do business experience additional significant data security incidents or fail to detect and appropriately respond to significant incidents, we could be exposed to additional government enforcement actions and private litigation. In addition, our guests could lose confidence in our ability to protect their information, discontinue using our RedCards or loyalty programs, or stop shopping with us altogether, which could adversely affect our reputation, sales, and results of operations.

The legal and regulatory environment regarding information security, cybersecurity, and data privacy is increasingly demanding and has enhanced requirements for using and treating personal data. Complying with data protection requirements, such as those imposed by a variety of state laws, may cause us to incur substantial costs, require changes to our business practices, limit our ability to obtain data used to provide a differentiated guest experience, and expose us to further litigation and regulatory risks, each of which could adversely affect our results of operations." *Target Corporation, Form 10-K filed on March 10, 2021 (SIC 5331—Retail—Variety Stores).*

- **"The Data Security Incident, and other information security incidents, could have numerous adverse effects on our business.**

  As a result of the Data Security Incident, we are a party to or have been named as a defendant in numerous lawsuits, primarily putative class actions, brought by consumers and others in the U.S. and Canada, one securities class action lawsuit in the U.S., three shareholder derivative lawsuits in the U.S., and one purported representative action brought by a purported consumer class in the U.K. We may be named as a party in additional lawsuits and other claims may be asserted by or on behalf of guests, customers, hotel owners, stockholders or others seeking monetary damages or other relief related to the Data Security Incident. A number of federal, state and foreign governmental authorities have also made inquiries, opened investigations, or requested information and/or documents related to the Data Security Incident, including under various data protection and privacy regulations. Responding to and resolving these lawsuits, claims and/or investigations has resulted in fines, such as the fine imposed by the Information Commissioner's Office in the United Kingdom (the ICO) as discussed in Note 8, and could result in material additional fines or remedial or other expenses. These fines and other expenses may not be covered by insurance. Governmental authorities investigating or seeking information about the Data Security Incident also may seek to impose undertakings, injunctive relief, consent decrees, or other civil or criminal penalties, which could, among other things, materially increase our data security costs or otherwise require us to alter how we operate our business. Significant management time and Company resources have been, and will continue to be, devoted to the Data Security Incident. Future publicity or developments related to the Data Security Incident, including as a result of subsequent reports or regulatory actions or developments, could have a range of other adverse effects on our business or prospects, including causing or contributing to loss of consumer confidence, reduced consumer demand, reduced enrollment and/or participation in our Loyalty Program, loss of development opportunities, and associate retention and recruiting difficulties. Insurance coverage designed to limit our exposure to losses such as those related to the Data Security Incident may not be sufficient or available to cover all of our expenses or other losses (including the final fine imposed by the ICO and any other fines or penalties) related to the Data Security Incident. In addition, following our March 31, 2020 announcement of an incident involving information for approximately 5.5 million guests that we believe may have been improperly accessed through an application using the login credentials of two franchise employees at a franchise property (the Unauthorized Application Access Incident), various governmental authorities opened investigations or requested information about the incident, and two lawsuits were filed against us related to the incident. The Unauthorized Application Access Incident or publicity related to it could negatively affect our business or reputation." *Marriott International, Inc., Form 10-K/A filed on April 2, 2021 (SIC 7011—Hotels & Motels).*

Cybersecurity Disclosures in the Business Section

Item 101(a) (17 C.F.R. § 229.101) of Regulation S-K requires a reporting company to describe the general development of its business and to disclose material information necessary to understand the general development of its business. For more information on the Business section requirements, including recent amendments thereto, see SEC Amends Disclosure Requirements for Business Sections, Legal Proceedings and Risk Factors and Form 10-K Drafting and Review — Overview of Major Items of Disclosure — Item 1. Description of Business. A number of public companies have disclosed in the Business section how cybersecurity risks pose a threat to their respective intellectual property, patents, and trade secrets. Many public companies pointed out the foreign and local government authorities' data security laws and regulations relevant to their operations, and how costly it is to comply with these issuances. Set forth below are some examples of cybersecurity disclosures in the Business section.

General Disclosure

- "As a provider of innovative network intelligence and security solutions for mobile and fixed service providers, we are particularly sensitive about the possibility of

cyber-attacks and data theft. A breach of our system could provide data information about us and the customers that our solutions protect. Further, we may be targeted by cyber-terrorists because we are an Israeli company. We are also aware of the material impact that an actual or perceived breach of our network may have on the market perception of our products and services and on our potential liability. In 2020 we have experienced cyber-attacks and breaches, that have been of a minor nature, with no material impacted our ongoing operations.

We are focused on instituting new technologies and solutions to assist in the prevention of potential and attempted cyber-attacks, as well as protective measures and contingency plans in the event of an existing attack. For instance, in our internal IT systems, we employ identity and access controls, product software designs and other security measures that we believe are less susceptible to cyber-attacks. We also continuously monitor our IT networks and systems for intrusions and regularly maintain our backup and protective systems. We have made certain updates to our IT infrastructure to enhance our ability to prevent and respond to such threats and we routinely test the infrastructure for vulnerabilities.

We conduct periodic trainings for our employees in this respect on phishing, malware and other cybersecurity risks to the Company. We also have mechanisms in place designed to ensure prompt internal reporting of potential or actual cybersecurity breaches, and maintain compliance programs to address the potential applicability of restrictions on trading while in possession of material, nonpublic information generally and in connection with a cybersecurity breach. Finally, our agreements with third parties also typically contain provisions that reduce or limit our exposure to liability." *Allot Ltd., Form 20-F filed on March 15, 2021 (SIC 3576—Computer Communications Equipment).*

- "We are a medical provider and comply with HIPAA and data sensitivity requirements as regulated by local and federal authorities. Our patient data is hosted, managed and secured with an approved Electronic Medical Record vendor. Cybersecurity is of paramount importance and our executive officers have implemented routine cyber breach insurance policies to protect our company from potential predatory initiatives to access patient and company data." *IMAC Holdings, Inc., Form 10-K filed on March 4, 2021 (SIC 8093—Services—Specialty Outpatient Facilities, NEC).*

Disclosures for Financial Services Companies

- "Cybersecurity is a high-priority item for legislators and regulators at the federal and state levels, as well as internationally. State and federal banking regulators have issued various policy statements and, in some cases, regulations, emphasizing the importance of technology risk management and supervision. Such policy statements and regulations indicate that financial institutions should design multiple layers of security controls to establish lines of defense and to ensure that their risk management processes also address the risk posed by compromised customer credentials, including security measures to reliably authenticate customers accessing internet-based services of the financial institution. A financial institution's management is expected to maintain sufficient business continuity planning processes to ensure the rapid recovery, resumption and maintenance of the institution's operations after a cyberattack involving destructive malware. A financial institution is expected to develop appropriate processes to enable recovery of data and business operations and address rebuilding network capabilities and restoring data if the institution or its critical service providers fall victim to this type of cyberattack. These requirements, including state regulatory rules such as the detailed and extensive cybersecurity rules issued in 2016 by the New York State Department of Financial Services, may cause us to incur significant additional compliance costs and in some cases may impact our growth prospects. Additionally, if we fail to observe federal or state regulatory guidance, we could be subject to various regulatory sanctions, including financial penalties.

  In the ordinary course of business, we rely on electronic communications and information systems to conduct our operations and store sensitive data. We employ an in-depth, layered, defensive approach that leverages people, processes and technology to manage and maintain cybersecurity controls. We also employ a variety of preventative and detective tools to monitor, block, and provide alerts regarding suspicious activity, as well as to report on any suspected advanced persistent threats. Notwithstanding the strength of our defensive measures, the threat from cyberattacks is severe, as attacks are sophisticated and increasing in volume and complexity, and attackers respond rapidly to changes in defensive measures. Our systems and those of our customers and third-party service providers are under constant threat, and it is possible that we or they could experience a significant event in the future that could adversely affect our business or operations. As cybersecurity threats continue to evolve, we may be required to expend

significant additional resources to continue to modify or enhance our protective measures or to investigate and remediate any information security vulnerabilities. Financial expenditures may also be required to meet regulatory changes in the information security and cybersecurity domains. Risks and exposures related to cybersecurity attacks are expected to remain high for the foreseeable future due to the rapidly evolving nature and sophistication of these threats, as well as the expanding use of internet banking, mobile banking and other technology-based products and services by us and our customers." *CapStar Financial Holdings, Inc., Form 10-K filed on March 5, 2021 (SIC 6022—State Commercial Banks).*

- "In the ordinary course of business, we rely on electronic communications and information systems to conduct our operations and to store sensitive data. We employ an in-depth, layered, defensive approach that leverages people, processes and technology to manage and maintain cybersecurity controls. We employ a variety of preventative and detective tools to monitor, block, and provide alerts regarding suspicious activity, as well as to report on any suspected persistent threats. Notwithstanding the strength of our defensive measures, the threat from cybersecurity attacks is severe, attacks are sophisticated and increasing in volume, and attackers respond rapidly to changes in defensive measures. While to date we have not experienced a significant compromise, significant data loss or any material financial losses related to cybersecurity attacks, our systems and those of our customers and third-party service providers are under constant threat and it is possible that we could experience a significant event in the future.

  The federal banking agencies have adopted guidelines for establishing information security standards and cybersecurity programs for implementing safeguards under the supervision of a banking organization's the board of directors. These guidelines, along with related regulatory materials, increasingly focus on risk management, processes related to information technology and operational resiliency, and the use of third parties in the provision of financial services.

  Risks and exposures related to cybersecurity attacks are expected to remain high for the foreseeable future due to the rapidly evolving nature and sophistication of these threats, as well as due to the expanding use of internet banking, mobile banking and other technology-based products and services by us and our customers." *Broadway Financial Corporation, Form 10-K filed on March 31, 2021 (SIC 6035—Savings Institution, Federally Chartered).*

- "In March 2015, the banking agencies issued two related statements regarding cybersecurity. One statement indicates that financial institutions should design multiple layers of security controls to establish lines of defense and to ensure that their risk management processes also address the risk posed by compromised customer credentials, including security measures to reliably authenticate customers accessing internet-based services of the financial institution. The other statement indicates that a financial institution's management is expected to maintain sufficient business continuity planning processes to ensure the rapid recovery, resumption and maintenance of the institution's operations after a cyber-attack involving destructive malware. A financial institution is also expected to develop appropriate processes to enable recovery of data and business operations and address rebuilding network capabilities and restoring data if the institution or its critical service providers fall victim to this type of cyber-attack. If we fail to observe the regulatory guidance, we could be subject to various regulatory sanctions, including financial penalties.

  In the ordinary course of business, we rely on electronic communications and information systems to conduct our operations and to store sensitive data. We employ an in-depth, layered, defensive approach that leverages people, processes and technology to manage and maintain cybersecurity controls. We employ a variety of preventative and detective tools to monitor, block, and provide alerts regarding suspicious activity, as well as to report on any suspected advanced persistent threats. Notwithstanding the strength of our defensive measures, the threat from cyberattacks is severe, attacks are sophisticated and increasing in volume, and attackers respond rapidly to changes in defensive measures. While to-date we have not experienced a significant compromise, significant data loss or any material financial losses related to cybersecurity attacks, our systems and those of our customers and third party service providers are under constant threat and it is possible that we could experience a significant event in the future. Risks and exposures related to cybersecurity attacks are expected to remain high for the foreseeable future due to the rapidly evolving nature and sophistication of these threats, as well as due to the expanding use of internet banking, mobile banking and other technology-based products and services by us and our customers.

  The SEC has also issued guidance on public company cybersecurity disclosures as well as ways for companies to enhance their cybersecurity preparedness and operational resiliency. Any SEC guidelines would be

in addition to notification and disclosure requirements under state and federal banking law and regulations." *HBT Financial, Inc., Form 10-K filed on March 12, 2021 (SIC 6022—State Commercial Banks).*

- "Cybersecurity presents significant challenges to the business community in general, as well as to the financial services industry. Increasingly, bad actors, both domestically and internationally, attempt to steal personal data and/or interrupt the normal functioning of businesses through accessing individuals' and companies' files and equipment connected to the Internet. Recently, intruders have become increasingly sophisticated and use deceptive methods to steal funds and personally identifiable information which they either take for their own purposes, release to the Internet, or hold for ransom. Regulators are increasingly requiring companies to provide more advanced levels of cybersecurity measures. We continue to maintain systems and ongoing planning measures to prevent any such attack from disrupting our services to clients as well as to prevent any loss of data concerning our clients, their financial affairs, and company-privileged information. We contract cybersecurity consultants as well as other vendors to oversee detection and defense from such attacks." *Siebert Financial Corp., Form 10-K filed on March 10, 2021 (SIC 6211—Security Brokers, Dealers & Flotation Companies).*

Disclosures Relating to Actual or Known Cybersecurity Breaches

- "On July 29, 2019, we announced that on March 22 and 23, 2019 an outside individual gained unauthorized access to our systems. This individual obtained certain types of personal information relating to people who had applied for our credit card products and to our credit card customers (the Cybersecurity Incident). We retained a leading independent cybersecurity firm that confirmed we correctly identified and fixed the specific configuration vulnerability exploited in the Cybersecurity Incident. We continue to invest significantly in cybersecurity and related risk management activities and expect to make additional investments as we continue to assess our cybersecurity program.

  During the year ended December 31, 2020, we incurred $66 million of incremental expenses related to the remediation of and response to the Cybersecurity Incident, offset by $39 million of insurance recoveries. To date, we have incurred $138 million of incremental expenses, offset by $73 million of insurance recoveries pursuant to the cyber risk insurance coverage we carry. These expenses mainly consist of customer notifications, credit monitoring, technology costs, and professional and legal support. We expect any further expenses, net of insurance, to be immaterial in future periods. We carry insurance to cover certain costs associated with a cyber risk event. This insurance has a total coverage limit of $400 million and is subject to a $10 million deductible, which was met in the third quarter of 2019, as well as standard exclusions. The expenses discussed in this paragraph do not include any amounts related to the matters described in 'Note 18—Commitments, Contingencies, Guarantees and Others.'

  Although the ultimate magnitude and timing of expenses or other impacts to our business or reputation related to the Cybersecurity Incident are uncertain, they may be significant, and some of the costs may not be covered by insurance. However, we do not believe that this incident will materially impact our strategy or our long-term financial health." *Capital One Financial Corporation, Form 10-K filed on February 25, 2021 (SIC 6021—National Commercial Banks).*

- "In 2017, we experienced a cybersecurity incident following a criminal attack on our systems that involved the theft of certain personally identifiable information of U.S., Canadian and U.K. consumers. Criminals exploited a software vulnerability in a U.S. website application to gain unauthorized access to our network. In March 2017, the U.S. Department of Homeland Security distributed a notice concerning the software vulnerability. We undertook efforts to identify and remediate vulnerable systems; however, the vulnerability in the website application that was exploited was not identified by our security processes. We discovered unusual network activity in late-July 2017 and upon discovery promptly investigated the activity. Once the activity was identified as potential unauthorized access, we acted to stop the intrusion and engaged a leading, independent cybersecurity firm to conduct a forensic investigation to determine the scope of the unauthorized access, including the specific information impacted. Based on our forensic investigation, the unauthorized access occurred from mid-May 2017 through July 2017. No evidence was found that the Company's core consumer, employment and income, or commercial reporting databases were accessed. On February 10, 2020, the U.S. Department of Justice announced that four members of the Chinese People's Liberation Army were indicted on criminal charges for their involvement in the 2017 cybersecurity incident.

  The Company has taken actions to provide consumers with tools to protect their credit data. Immediately following the announcement of the 2017 cybersecurity

incident, the Company devoted substantial resources to notify people of the incident and to provide free services to assist people in monitoring their credit and identity information. Since then, the Company has been focused on implementing significant improvements to its data security systems, technology platforms and risk management processes, in an effort to underpin its business strategy." *Equifax Inc., Form 10-K filed on February 25, 2021 (SIC 7320—Services—Consumer Credit Reporting, Collection Agencies).*

Disclosure regarding Ongoing Litigation Related to Cybersecurity Breaches

"The Company is also exposed to risks related to information security arising from the information technology systems and operations of third parties, including those of the Company's vendors and partners. For example, on May 14, 2019, Retrieval-Masters Credit Bureau, Inc. d/b/a/ American Medical Collections Agency (AMCA), an external collection agency, notified the Company about a security incident AMCA experienced that may have involved certain personal information about some of the Company's patients (the AMCA Incident). The Company referred patient balances to AMCA only when direct collection efforts were unsuccessful. The Company's systems were not impacted by the AMCA Incident. Upon learning of the AMCA Incident, the Company promptly stopped sending new collection requests to AMCA and stopped AMCA from continuing to work on any pending collection requests on behalf of the Company. AMCA informed the Company that it appeared that an unauthorized user had access to AMCA's system between August 1, 2018 and March 30, 2019, and that AMCA could not rule out the possibility that personal information on AMCA's system was at risk during that time period. Information on AMCA's affected system from the Company may have included name, address, and balance information for the patient and person responsible for payment, along with the patient's phone number, date of birth, referring physician, and date of service. The Company was later informed by AMCA that health insurance information may have been included for some individuals, and because some insurance carriers utilize the Social Security Number as a subscriber identification number, the Social Security Number for some individuals may also have been affected. No ordered tests, laboratory test results, or diagnostic information from the Company were in the AMCA affected system. The Company notified individuals for whom it had a valid mailing address. For the individuals whose Social Security Number was affected, the notice included an offer to enroll in credit monitoring and identity protection services that will be provided free of charge for 24 months. The Company has incurred, and expects to continue to incur, costs related to the AMCA Incident. The Company is involved in pending and threatened litigation related to the AMCA Incident, as well as various government and regulatory inquiries and processes. [Additional information about the AMCA Incident were provided in the Notes to the Consolidated Financial Statements.]" *Laboratory Corp of America Holdings, Form 10-K filed on February 25, 2021 (SIC 8071—Services—Medical Laboratories).*

Cybersecurity Disclosures in the MD&A Section

Item 303(b) (17 C.F.R. § 229.303) of Regulation S-K requires a discussion of a company's financial condition and changes in its financial condition and results of operations, including any known trends, commitments, events, or uncertainties that will or are reasonably likely to have a material impact on, the company's business, financial position, or results of operations. For further information on the MD&A section, including recent amendments, see Management's Discussion and Analysis of Financial Condition and Results of Operations, SEC Amends MD&A and Other Financial Disclosure Requirements: Client Alert Digest, Management's Discussion and Analysis (MD&A) Resource Kit, and Management's Discussion and Analysis Section Drafting Checklist. Some companies included disclosures regarding possible cybersecurity incidents, and the potential impact of such incidents, in their MD&A A few companies disclosed financial losses and cybersecurity-related costs when there were known or ongoing cybersecurity incidents. Set forth below are some examples of cybersecurity breach disclosures in the MD&A section of periodic reports.

General Disclosure

- "The number and sophistication of attempts to disrupt or penetrate our systems—sometimes referred to as hacking, cyber fraud, cyberattacks, or other similar names—continues to grow. To combat the ever-increasing sophistication of cyberattacks, we are continuously improving methods for detecting and preventing attacks. In addition, we have implemented policies and procedures and developed specific training for our employees and elevated our oversight and internal reporting to the Board and respective committees. Further, we regularly engage independent third-party cyber experts to test for vulnerabilities in our environment. We also conduct our own internal simulations and tabletop exercises as well as participate in financial sector-specific exercises. We have engaged consultants at both the strategic level and at

the technology implementation level to assist us in better managing this critical risk.

While we have significant internal resources, policies and procedures designed to prevent or limit the effect of the possible failure, interruption or security breach of our information systems, we have experienced security breaches due to cyberattacks in the past and there can be no assurance that any such failure, interruption or security breach will not occur in the future, or, if they do occur, that they will be adequately addressed. It is impossible to determine the potential effects of these events with any certainty, but any such breach could result in material adverse consequences for us and our customers." *Zions Bancorporation, National Association, Form 10-K filed on February 25, 2021 (SIC 6021—National Commercial Banks).*

Cybersecurity Risk Management Disclosure

- "We maintain comprehensive Cyber Incident Response Plans, and we devote significant time and resources to maintaining and regularly updating our technology systems and processes to protect the security of our computer systems, software, networks, and other technology assets against attempts by third parties to obtain unauthorized access to confidential information, destroy data, disrupt or degrade service, sabotage systems, or cause other damage. We and many other U.S. financial institutions have experienced distributed denial-of-service attacks from technologically sophisticated third parties. These attacks are intended to disrupt or disable online banking services and prevent banking transactions. We also periodically experience other attempts to breach the security of our systems and data. These cyberattacks have not, to date, resulted in any material disruption of our operations or material harm to our customers, and have not had a material adverse effect on our results of operations.

  Cyberattack risks may also occur with our third-party technology service providers, and may result in financial loss or liability that could adversely affect our financial condition or results of operations. Cyberattacks could also interfere with third-party providers' ability to fulfill their contractual obligations to us. High-profile cyberattacks have targeted retailers, credit bureaus, and other businesses for the purpose of acquiring the confidential information (including personal, financial, and credit card information) of customers, some of whom are customers of ours. We may incur expenses related to the investigation of such attacks or related to the protection of our customers from identity theft as a result of such attacks. In 2020, many companies and U.S. government organizations were victims of a sophisticated and targeted supply chain attack on the SolarWinds Orion software. While Key does not utilize the SolarWinds software products, some of our vendors do. We may incur expenses to enhance our systems or processes to protect against cyber or other security incidents. Risks and exposures related to cyberattacks are expected to remain high for the foreseeable future due to the rapidly evolving nature and sophistication of these threats, as well as due to the expanding use of Internet banking, mobile banking, and other technology-based products and services by us and our clients. See the risk factor entitled 'Our information systems may experience an interruption or breach in security' in Part 1, Item 1A. Risk Factors for additional information on risks related to information security.

  As described in more detail in 'Risk Management – Overview' in Item 7 of this report, the Board serves in an oversight capacity ensuring that Key's risks are managed in a manner that is effective and balanced and adds value for the shareholders. The Board's Risk Committee has primary oversight for enterprise-wide risk at KeyCorp, including operational risk (which includes cybersecurity). The Risk Committee reviews and provides oversight of management's activities related to the enterprise-wide risk management framework, including cyber-related risk. Board members are updated on cybersecurity matters at each regularly-scheduled Board meeting. The ERM Committee, chaired by the Chief Executive Officer and comprising other senior level executives, is responsible for managing risk (including cyber-related risk) and ensuring that the corporate risk profile is managed in a manner consistent with our risk appetite. The ERM Committee reports to the Board's Risk Committee." *KeyCorp, Form 10-K filed on February 22, 2021 (SIC 6021—National Commercial Banks).*

- "As a global provider of satellite technologies and services, internet services and communications equipment and networks, we may be prone to more targeted and persistent levels of cyber-attacks than other businesses. These risks may be more prevalent as we continue to expand and grow our business into other areas of the world outside of North America, some of which are still developing their cybersecurity infrastructure maturity. Detecting, deterring, preventing and mitigating incidents caused by hackers and other parties may result in significant costs to us and may expose our customers to financial or other harm that have the potential to significantly increase our liability.

  Due to the COVID-19 pandemic, a large portion of our workforce has been working remotely and we expect certain portions of our workforce to continue to do

so from time to time. While we have cybersecurity risk management tools to help protect our technology, information and networks that our employees access remotely, we cannot guarantee the security of the network that they will be using, the security status of the other non-company managed devices that might be on the network to which they are connected or the devices or networks used by third parties with whom our employees conduct business, such as customers, suppliers, vendors and other persons. Additionally, there continues to be a significant amount of COVID-19 related cyber-fraud and phishing attacks that continue to target our employees, vendors, suppliers, customers and others. Accordingly, we increased our cybersecurity efforts and resources as a result of the COVID-19 pandemic.

We treat cybersecurity risk seriously and are focused on maintaining the security of our and our partners' systems, networks, technologies and data. We regularly review and revise our relevant policies and procedures, invest in and maintain internal resources, personnel and systems and review, modify and supplement our defenses through the use of various services, programs and outside vendors. Additionally, we provide resources to assist employees in better securing their home networks and remote connections. We also maintain agreements with third party vendors and experts to assist in our remediation and mitigation efforts if we experience or identify a material incident or threat. In addition, senior management and the Audit Committee of our Board of Directors are regularly briefed on cybersecurity matters. EchoStar also maintains agreements with third party vendors and experts to assist in our remediation and mitigation efforts if we experience or identify a material incident or threat. In addition, senior management and the Audit Committee of EchoStar's Board of Directors are regularly briefed on cybersecurity matters.

On December 8, 2020, the cyber security company FireEye announced that they detected a sophisticated nation state level cyber campaign that targeted FireEye, other public and private companies, and government organizations. FireEye reported that the attack against them was facilitated through the Orion IT management software owned by a company called SolarWinds. Based on information from FireEye, we reviewed all instances of SolarWinds software in use at the Company and have determined that the version we are using is not susceptible to the malware within the version that is compromised. We continue to receive information about these breaches from the U.S. government and private security firms, and we use this data to update our defense systems and to investigate our own networks for compromise. We will continue to update our systems as more information comes to light in reference to this adversary and their actions." *Hughes Satellite Systems Corporation, Form 10-K filed on February 23, 2021 (SIC 4899—Communications Services, NEC).*

- "In an effort to reduce the likelihood and severity of cybersecurity incidents, we have established a comprehensive cybersecurity program designed to protect and preserve the confidentiality, integrity and availability of our information systems. The Board, the Audit Committee, Industrial Operations Committee and senior management receive frequent reports on such topics as personnel and resources to monitor and address cybersecurity threats, technological advances in cybersecurity protection, rapidly evolving cybersecurity threats that may affect our Company and industry, cybersecurity incident response and applicable cybersecurity laws, regulations and standards, as well as collaboration mechanisms with intelligence and enforcement agencies and industry groups, to assure timely threat awareness and response coordination.

  [. . .] PSEG also maintains physical security measures to protect its Operational Technology systems, consistent with a defense in depth and risk-tiered approach. Such physical security measures may include access control systems, video surveillance, around-the-clock command center monitoring, and physical barriers (such as fencing, walls, and bollards). Additional features of PSEG's physical security program include threat intelligence, insider threat mitigation, background checks, a threat level advisory system, a business interruption management model, and active coordination with federal, state, and local law enforcement officials. See Regulatory Issues-Federal for a discussion on physical reliability standards that the NERC has promulgated.

  In addition, we are subject to federal and state requirements designed to further protect against cybersecurity threats to critical infrastructure, as discussed below." *Public Service Enterprise Group Incorporated, Form 10-K filed on March 1, 2021 (SIC 4931—Electric & Other Services Combined).*

Disclosures Relating to Actual or Known Cybersecurity Breaches

- "In May 2020, we were affected by a ransomware cyber-attack that temporarily disrupted production at our Atchison facilities. Our financial information was not affected and there is no evidence that any sensitive or confidential company, supplier, customer or employee data was improperly accessed or extracted from our network. We estimate that the ransomware attack

adversely impacted gross profit by $1,728, primarily as a result of the business interruption. We have insurance related to this event and partially recovered $633 in December 2020 as reduction of Cost of sales. We are currently seeking further recovery related to this event. Following the attack, we implemented a variety of measures to further enhance our cybersecurity protections and minimize the impact of any future attack." *MGP Ingredients Inc., Form 10-K filed on February 25, 2021 (SIC 5180—Wholesale—Beer, Wine & Distilled Alcoholic Beverages).*

- "As we previously disclosed on December 9, 2019 on a Form 8-K filed with the Securities and Exchange Commission (SEC), we detected a cyberattack on our network on the evening of December 5, 2019 PST and immediately took affected systems offline as part of our comprehensive response to contain the activity (December 2019 Cyberattack). The virus was targeted at Windows-based systems and did not attack our global ERP system (SAP) and other non-Windows-based systems. Critical systems were back online within a few days of the incident. As part of our in-depth investigation into this incident, we engaged outside cyber security experts to assist us with investigation and remediation efforts. We have found no evidence of unauthorized transfer or misuse of personal data, and there is no indication that customer systems were affected.

  We have insurance coverage for costs resulting from cyberattacks. We did not pay a ransom in connection with this incident." *Bio-Rad Laboratories, Inc., Form 10-K filed on February 16, 2021 (SIC 3826—Laboratory Analytical Instruments).*

- "The Company experienced two intrusions to its digital systems, one in May 2016 and one in January 2017. Hackers and related organized criminal groups obtained unauthorized access to certain customer accounts. The attacks disabled certain systems protections, including limits on the number, amount, and frequency of ATM withdrawals. The attacks resulted in the theft of funds disbursed through ATMs. In the May 2016 attack, hackers accessed customer funds and in the January 2017 intrusion, the hackers artificially inflated account balances and did not access customer funds. The Company notified all affected customers, and restored all funds so that no customer experienced a loss. The Company retained a nationally recognized firm to investigate and remediate the May 2016 intrusion and a separate nationally recognized firm to investigate and remediate the January 2017 intrusion. The Company adopted and implemented all of the recommendations provided through the investigations.

  The financial impact of the attacks include the amount of the theft, as well as costs of investigation and remediation. The theft of funds totaled $570 in the May 2016 attack and $1,838 in the January 2017 attack. The Company recognized an estimated loss of $347 in 2016, and $2,010 in 2018. Costs for investigation, remediation, and legal consultation totaled $157 in 2019, $224 in 2018 and $407 in 2017. The Company's litigation against the insurance carrier was settled during the first quarter of 2019, subject to a non-disclosure agreement. There has been no litigation against the Company to date associated with the breaches.

  We have deployed a multi-faceted approach to limit the risk and impact of unauthorized access to customer accounts and to information relevant to customer accounts. We use digital technology safeguards, internal policies and procedures, and employee training to reduce the exposure of our systems to cyber-intrusions. However, it is not possible to fully eliminate exposure. The potential for financial and reputational losses due to cyber-breaches is increased by the possibility of human error, unknown system susceptibilities, and the rising sophistication of cyber-criminals to attack systems, disable safeguards and gain access to accounts and related information. The Company maintains insurance which provides a degree of coverage depending on the nature and circumstances of any cyber penetration but cannot be relied upon to reimburse fully the Company for all losses that may arise. The Company has adopted new protections and invested additional resources to increase its security." *National Bankshares Inc., Form 10-K filed on March 18, 2021 (SIC 6021—National Commercial Banks).*

- "On November 30, 2018, we announced a data security incident involving unauthorized access to the Starwood reservations database (the Data Security Incident). The Starwood reservations database is no longer used for business operations.

  In July 2019, the ICO issued a formal notice of intent under the U.K. Data Protection Act 2018 (the U.K. DPA) proposing a fine in the amount of £99 million against the Company in relation to the Data Security Incident. In October 2020, the ICO issued a final decision under the U.K. DPA, which includes a fine of £18.4 million. The Company did not appeal the ICO's decision, but has made no admission of liability in relation to the decision or the underlying allegations. In 2019, we expensed $65 million for this loss contingency, in the 'Restructuring and merger-related charges' caption of our Income Statements, based on the fine initially proposed by the ICO in July 2019 and the ongoing proceeding. In 2020,

we recorded a $39 million reversal of expense, based on the ICO's issuance of the final decision. We paid a portion of the ICO fine in the 2020 fourth quarter, and the remainder is payable over the next two years. Our accrual for this loss contingency, which we present in the 'Accrued expenses and other' and 'Other noncurrent liabilities' captions of our Balance Sheets, was $65 million at year-end 2019 and $17 million at year-end 2020. See Note 8 for additional information.

We are currently unable to estimate the range of total possible financial impact to the Company from the Data Security Incident in excess of the expenses already incurred. However, we do not believe this incident will impact our long-term financial health. Although our insurance program includes coverage designed to limit our exposure to losses such as those related to the Data Security Incident, that insurance may not be sufficient or available to cover all of our expenses or other losses (including fines and penalties) related to the Data Security Incident. As we expected, the cost of such insurance again increased for our current policy period, and the cost of such insurance could continue to increase for future policy periods. We expect to incur significant expenses associated with the Data Security Incident in future periods, primarily related to legal proceedings and regulatory investigations (including possible additional fines and penalties), increased expenses and capital investments for information technology and information security and data privacy, and increased expenses for compliance activities and to meet increased legal and regulatory requirements. See Note 8 for additional information related to expenses incurred in 2020 and 2019, insurance recoveries, and legal proceedings and governmental investigations related to the Data Security Incident." *Marriott International, Inc., Form 10-K/A filed on April 2, 2021 (SIC 7011—Hotels & Motels).*

- "In August 2019, the Company experienced a network security incident caused by malware that prevented access to several of the Company's information technology systems and data. Stores remained open and operating throughout the incident, but the Company utilized manual back-up processes for approximately six days. The Company estimated the disruption caused by the event negatively impacted total revenue for the third quarter of 2019 in the range of approximately $6 million to $8 million with an attendant reduction in gross margin. The Company maintains cybersecurity and other insurance coverage and received an initial recovery from insurance in excess of $2 million in 2019. As of December 31, 2019, the Company recorded approximately $0.8 million as a receivable related to further anticipated insurance recovery. The receivable did not include any potential business interruption recovery or voluntary gains. It was recorded in 'Other Current Assets' on the Consolidated Balance Sheet as of December 31, 2019 and was collected during 2020. In 2020 the Company recorded $2.5 million from the final settlement of the business interruption insurance claim in SG&A during the third quarter of 2020." *Lumber Liquidators Holdings, Inc., Form 10-K filed on March 2, 2021 (SIC 5211—Retail—Lumber & Other Building Materials Dealers).*
- "On December 14, 2020, we announced that we had been the victim of a cyberattack on our Orion Software Platform and internal systems, or the 'Cyber Incident.' Together with outside security professionals and other third parties, we are conducting investigations into the Cyber Incident which are on-going.

  Our investigations to date revealed that as part of this attack, malicious code, or Sunburst, was injected into builds of our Orion Software Platform that we released between March 2020 and June 2020. If present and activated in a customer's IT environment, Sunburst could potentially allow an attacker to compromise the server on which the Orion Software Platform was installed. We have not located Sunburst in any of our more than seventy non-Orion products and tools.

  We released remediations for the versions of our Orion Software Platform known to be affected by Sunburst and have taken and continue to take extensive efforts to support and protect our customers. In addition, we shared our proprietary code with industry researchers to enable them to validate a 'kill-switch' that is believed to have rendered Sunburst inert.

  The Orion Software Platform is installed 'on-premises' within customers' IT environments, so we are unable to determine with specificity the number of customers that installed an affected version or that were compromised as a result of Sunburst. We believe the actual number of customers that could have installed an affected version of the Orion Software Platform to be fewer than 18,000. Based on our discussions with customers and our investigations into the nature and function of Sunburst and the tradecraft of the threat actor, we believe the number of organizations which were exploited by the threat actors through Sunburst to be substantially fewer than the number of customers that may have installed an affected version of the Orion Platform.

  It has been widely reported that, due to its nature, sophistication and operational security, this 'supply-chain' cyberattack was part of a broader nation-state level cyber operation designed to target public and private sector organizations. As of the date hereof, we have

not independently attributed the Cyber Incident to any specific threat actor.

Through our investigations into the Cyber Incident, we hope to understand it better, apply our findings to further adapt and enhance our security measures across our systems and our software development and build environments and share our findings and adaptations with our customers, government officials and the technology industry more broadly to help them better understand and protect against these types of attacks in the future. We refer to these adaptations and enhancements as 'Secure by Design.'

As described below, we have incurred and expect to incur significant costs related to the Cyber Incident. We are also party to lawsuits and the subject of governmental investigations related to the Cyber Incident. See Part I, Item 1A. Risk Factors – Risks Related to the Cyber Incident and Note 16. Commitments and Contingencies in the Notes to Consolidated Financial Statements included in Item 8 of Part II of this Annual Report on Form 10-K for more information regarding these lawsuits and investigations." *SolarWinds Corp., Form 10-K filed on March 1, 2021 (SIC 7372 Services—Prepackaged Software).*

Disclosure regarding Internal Control over Financial Reporting Issues or Material Weaknesses Resulting from Failure to Address Cybersecurity Risks

- "On April 20, 2020, we announced a security incident involving a Maze ransomware attack. Based on numerous remediation steps that have been undertaken and our continued monitoring of our environment, we believe we have contained the attack and eradicated remnants of the attacker activity from our environment. Based on our investigation, we believe the attack principally impacted certain of our systems and data. The attack resulted in unauthorized access to certain data and caused significant disruption to our business. This included the disabling of some of our systems and disruption caused by our taking certain other internal systems and networks offline as a precautionary measure. The attack compounded the challenges we faced in enabling work-from-home arrangements during the COVID-19 pandemic and resulted in setbacks and delays to such efforts. The impact to clients and their responses to the security incident varied. Some clients experienced no disruption. As to other clients, we experienced service disruptions due to our reliance on certain of the impacted systems and networks to perform work for clients and the impact to our systems and networks supporting work-from-home capabilities. The systems that comprise the technology platforms that support our business process-as-a-service solutions were not impacted. Most clients maintained connectivity with our network, allowing us to continue to provide service, but some clients opted to suspend our access to their networks as a security precaution. In this circumstance, we are unable to continue providing services via client networks until access is restored. We engaged leading outside forensics and cybersecurity experts, launched a comprehensive containment and remediation effort and forensic investigation, restored the security of our internal systems and networks and are adopting various enhancements to the security of our systems and networks. We also notified and are coordinating with law enforcement." *Cognizant Technology Solutions Corporation, Form 10-Q filed on July 30, 2020 (SIC 7371—Services—Computer Programming Services).*

Disclosure regarding Ongoing Litigation Related to Cybersecurity Breaches

- "As a result of the 2017 cybersecurity incident, we were subject to a significant number of proceedings and investigations as described in Part I, 'Item 3. Legal Proceedings' in this Form 10-K. We did not record any settlement expenses related to the resolution of these proceedings and investigations for the twelve months ended December 31, 2020. We recorded expenses, net of insurance recoveries, of $800.9 million in other current liabilities and selling, general, and administrative expenses in our Consolidated Balance Sheets and Statements of Income (Loss), respectively, as of and for the twelve months ended December 31, 2019, exclusive of our legal and professional services expenses and net of insurance recoveries. The amount accrued represents our best estimate of the liability related to these matters. The Company will continue to evaluate information as it becomes known and adjust accruals for new information and further developments in accordance with ASC 450-20-25." *Equifax Inc., Form 10-K filed on February 25, 2021 (SIC 7320—Services—Consumer Credit Reporting, Collection Agencies).*
- "As a result of the Cyber Incident, we are subject to numerous lawsuits and investigations or inquiries as described in Note 16. Commitments and Contingencies in the Notes to Consolidated Financial Statements included in Item 8 of Part II of this Annual Report on Form 10-K. While we will incur costs and other expenses associated with these proceedings and investigations, it is not possible to estimate the amount of any loss or range of possible loss that might result from adverse

judgments, settlements, penalties or other resolutions of such proceedings and investigations based on the early stage thereof, the fact that alleged damages have not been specified, the uncertainty as to the certification of a class or classes and the size of any certified class, as applicable, and the lack of resolution on significant factual and legal issues. We will continue to evaluate information as it becomes known and will record an estimate for losses at the time or times when it is both probable that a loss has been incurred and the amount of the loss is reasonably estimable. [Additional information about the Cyber Incident was provided in the Notes to the Consolidated Financial Statements.]" *SolarWinds Corp., Form 10-K filed on March 1, 2021 (SIC 7372 Services—Prepackaged Software).*

For a form of cybersecurity risk factor, including drafting notes and further practical guidance, see Cybersecurity Risk Factor.

Market Outlook

Cybersecurity Disclosure Enhancements

Cybersecurity risks and their resulting business and financial consequences continue to evolve as technology continues to improve through time. Investors and regulators require more robust disclosures on cybersecurity risks and incidents. The following steps may help you in preparing the required cybersecurity disclosures in SEC-filed documents:

- **Ascertain if the company is or is reasonably likely to be affected by new or existing cybersecurity threats.** As securities, financial markets, market participants, and their vendors continue to increase reliance on technology and digital connections, each reporting company should aggressively determine whether and how its cybersecurity risk profile and operational resiliency are vulnerable to cybersecurity threats. Cybersecurity threats originate from many sources globally and include malwares that take the form of computer viruses, ransomware, worms, Trojan horses, spyware, adware, scareware, rogue software, and programs that act against the computer user.
- **Develop company-specific disclosures of material cybersecurity risks.** A public company should objectively assess whether the cybersecurity threats have or will probably have a material effect on the integrity and security of its computers, programs, software, servers, or computer network. If material, the company should disclose the resulting cybersecurity risks to the company, the cybersecurity threats' impact on market systems and customer data protection, and how the company intends to comply with legal and regulatory obligations under the securities laws applicable to it. While a public company may be guided by cybersecurity disclosures of other public companies, the reporting company should particularly disclose how these cybersecurity risks and incidents might impact the company, its management, operations, contractors, and prospects. A company should refrain from adding boilerplate cybersecurity disclosure that is not meaningful to investors, and should instead provide additional cybersecurity disclosures to underscore its special circumstances. Such special circumstances could include having a strong e-commerce presence, outsourcing business functions, handling its own business and personnel data with a platform for online financial transactions, collecting and storing of health-related records of its clientele with public safety concerns due to the nature of the industry the company is in, or whether the company is covered by insurance for cybersecurity events.
- **Disclose the costs associated with cybersecurity efforts.** Companies should consider disclosing in the MD&A section and in the financial statements the costs of managing and combating cybersecurity risks, as well as the expenses related to addressing ongoing cybersecurity threats and breaches. These costs include regulatory investigation and litigation expenses, loss or depreciation of intellectual properties, and costs to maintain and enhance operational resiliency.
- **Balance the particularity requirement with safeguarding sensitive information.** Like other disclosures, disclosure of cybersecurity risks and incidents requires a fine balance between particularity and the need to protect sensitive information that might serve as a potential hacker's road map for future cyberattacks. Public companies are not required to make detailed disclosures that could jeopardize their cybersecurity efforts or aggravate their cybersecurity risks.
- **Furnish timely and ongoing disclosures of cybersecurity incidents.** Once a material cybersecurity incident happens, a company should provide notice to investors (e.g., through a current report on Form 8-K or 6-K) within the required time frame. The notice should disclose accurate and sufficient material information about the cybersecurity threat or breach and the company's intended remedial measures in addressing it. An ongoing internal or external investigation should not by itself delay disclosing the occurrence of a material event. For further information on timely disclosure, see Duties to Disclose and Update Material Information.

- **Disclose cybersecurity internal control assessment and operational resiliency enhancement efforts.** SEC expects public companies to maintain and monitor effective internal controls over financial reporting and to recalibrate these controls as cybersecurity risks continue to evolve. Based on OCIE's guide, a reporting company should also disclose how it manages cybersecurity risks and enhances operational resiliency in the areas of governance and risk management, access rights and controls, data loss prevention, mobile security, incident response and resiliency, vendor management, and training and awareness.

Anna T. Pinedo, Partner, Mayer Brown LLP

Anna T. Pinedo is a partner in Mayer Brown's New York office and a member of the Corporate & Securities practice. She concentrates her practice on securities and derivatives. Anna represents issuers, investment banks/financial intermediaries and investors in financing transactions, including public offerings and private placements of equity and debt securities, as well as structured notes and other hybrid and structured products.

She works closely with financial institutions to create and structure innovative financing techniques, including new securities distribution methodologies and financial products. She has particular financing experience in certain industries, including technology, telecommunications, healthcare, financial institutions, REITs and consumer finance. Anna has worked closely with foreign private issuers in their securities offerings in the United States and in the Euro markets. She also works with financial institutions in connection with international offerings of equity and debt securities, equity- and credit-linked notes, and hybrid and structured products, as well as medium term note and other continuous offering programs.

In the derivatives area, Anna counsels a number of major financial institutions acting as dealers and participants in the commodities and derivatives markets. She advises on structuring issues as well as on regulatory issues, including those arising under the Dodd-Frank Act. Her work focuses on foreign exchange, equity and credit derivatives products, and structured derivatives transactions. Anna has experience with a wide range of transactions and structures, including collars, swaps, forward and accelerated repurchases, forward sales, hybrid preferred stock and off-balance sheet structures. She also has advised derivatives dealers regarding their Internet sites and other Internet and electronic signature/delivery issues, as well as on compliance matters.

Gonzalo D.V. Go III, Associate, Mayer Brown LLP

Gonzalo D.V. Go III is an associate in Mayer Brown's Corporate & Securities practice. He advises issuers on shelf registration statements, medium term note programs and issuances exempt from registration under Rule 144A, Regulation S and Section 3(a)(2) of the Securities Act. He advises issuers, investment banks and sponsors in public and private offerings of equity and debt securities, including initial public offerings; de-SPAC and Up-C business combinations; follow-on offerings; investment grade debt offerings and securitizations. He also assists public companies with stock exchange listing applications, maintenance and transfers; securities law reporting and compliance requirements such as Forms 10-K, 10-Q and 8-K, and Section 16 filings; and general corporate governance matters, including preparation and review of resolutions, minutes, meeting agendas and relevant corporate policies and processes.

G earned his LLM from Columbia Law School, where he served as a student senator and graduated as the class speaker, a Harlan Fiske Stone scholar and a recipient of the Parker School Recognition of Achievement in International and Comparative Law. He earned his JD, with honors, from the Ateneo Law School and his BS in Accountancy, with honors, from De La Salle University.

G's prior professional experiences include being (i) a capital markets associate in another global law firm in New York, (ii) an associate general counsel of Jollibee Foods Corporation, a multinational fast-food chain headquartered in the Philippines, where he gained extensive experience in managing legal risks in various business activities such as business development and expansion, customer relations, operations, real estate, franchising, marketing, human resources, purchasing, finance, corporate communications, tax and government relations, (iii) a member of the faculty of the Ateneo Law School and (iv) a tax associate in SyCip Salazar Hernandez & Gatmaitan, a top tier law firm in the Philippines. G is also a lawyer and a certified public accountant in the Philippines.

Nicole Cors, Associate, Mayer Brown LLP

Nicole Cors is an associate in Mayer Brown's Chicago office and a member of the Corporate & Securities practice.

Felix R. Zhang, Associate, Mayer Brown LLP

Felix Zhang is an associate in Mayer Brown's Washington DC office and a member of the Corporate & Securities practice.

Felix received his JD from New York University School of Law, where he served as the Managing Editor of the *New York University Journal of Law and Business*, his MA from Johns Hopkins University, and his BA from Pomona College.