Market Trends 2019/20: Cybersecurity Disclosures

A Lexis Practice Advisor® Practice Note by Anna T. Pinedo, Gonzalo Go, and Nicole Cors, Mayer Brown LLP

Anna T. Pinedo
Mayer Brown LLP

Gonzalo Go
Mayer Brown LLP

Nicole Cors
Mayer Brown LLP

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

For further information on public company disclosure in general, see Public Company Periodic Reporting and Disclosure Obligations and Periodic and Current Reporting Resource Kit. For other market trends articles covering various capital markets and corporate governance topics, see Market Trends.

On October 16, 2018, the Securities and Exchange Commission (SEC) released a report pursuant to Section 21(a) of the Securities Exchange Act of 1934 (the Exchange Act) detailing its investigation of several public companies that were victims of cybersecurity-related frauds. 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) of the Exchange Act to devise and maintain a sufficient system of internal accounting controls. On December 6, 2018, SEC Chairman Jay Clayton, in his speech, highlighted cybersecurity risks as one of the prominent challenges the SEC faces. 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 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 preventative measures and insurance; and the costs associated with cybersecurity incidents, including remedial measures, investigations, responding to regulatory actions, and addressing litigation.

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. OCIE classified their 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.

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 litigations.

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 list of risks applicable to almost any company. These disclosures simply included general statements about cybersecurity risks and incidents but did not particularly disclose how these cybersecurity risks and incidents might impact the company, its management, operations, contractors, 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 article identifies some cybersecurity-related disclosures that offer more detailed discussions of effects.

Cybersecurity Disclosures in the Risk Factor Section

Item 503(c) (17 C.F.R. § 229.503) 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 2016/17: 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 Registration Statement and Preliminary Prospectus Preparations for an IPO. A majority of companies choose to disclose cybersecurity risks in the Risk Factor 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 service companies, may want to enhance their disclosures by discussing the relevant regulatory development on cybersecurity. When a cybersecurity breach occurs, a company typically discloses such incident together with the remedial actions the company is planning to undertake, the estimated losses arising from the breach, and if there are litigation and regulatory actions or other consequences associated with the cybersecurity breach. Some examples of cybersecurity disclosures in the Risk Factor section are set forth below.

General Disclosure on Cybersecurity Risks

- **"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, 2020 (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, 2020 (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 March 13, 2020 (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 April 10, 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 reducing 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 POS 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 13, 2020 (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. Such cybersecurity breaches may be the result of unauthorized activity by our employees or contractors or malware, hacking, business email compromise, phishing or other cyberattacks directed by third parties. While we have implemented measures to protect our information and data, 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. 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-Q filed May 1, 2020 (SIC 2834—Pharmaceutical Preparations)*

Disclosures Relating to Actual or Known Cybersecurity Breaches and Remedial Measures

- **"A failure of our information technology infrastructure or a breach of our information security systems, networks or processes may materially adversely affect our business.**

  [. . .] We have been, and in the future may be, subject to cybersecurity and malware attacks and other intentional hacking. Any failure to identify and address such defects or errors or prevent a cyber- or malware-attack could result in service interruptions, operational difficulties, loss of revenues or market share, liability to our customers or others, the diversion of corporate resources, injury to our reputation and increased service and maintenance costs. In September 2019, we suffered a server and applications quarantine caused by a malware attack, which negatively impacted our revenue for the year ended December 31, 2019, by approximately $10.9 million and caused delays in invoicing, which led to increased costs, including bad debt. In the fourth quarter of 2019, we filed insurance claims to attempt to recover the impact on lost business.

  On other occasions, we have experienced other phishing attacks, social engineering and wire fraud affecting our employees and suppliers, which has resulted in leakage of personally identifiable information and loss of funds. Addressing such issues could prove to be impossible or very costly and responding to resulting claims or liability could similarly involve substantial cost. In addition, recently, there has also been heightened regulatory and enforcement focus on data protection in the United States and abroad, and failure to comply with applicable U.S. or foreign data protection regulations or other data protection standards may expose us to litigation, fines, sanctions or other penalties, which could harm our reputation and adversely impact our business, results of operations and financial condition.

  We have invested and continue to invest in technology security initiatives, employee training, information technology risk management and disaster recovery plans. The development and maintenance of these measures is costly and requires ongoing monitoring and updating as technologies change and efforts to overcome security measures become increasingly more sophisticated. Despite our efforts, we are not fully insulated from data breaches, technology disruptions or data loss, which could adversely impact our competitiveness and results of operations." *Roadrunner Transportation Systems, Inc., Form 10-K filed on March 30, 2020 (SIC 4731—Arrangement of Transportation of Freight & Cargo)*

- **"We are exposed to cyber-attacks and data breaches, including the risks and costs associated with protecting our systems and maintaining integrity and security of our business information, as well as personal data of our guests, employees and business partners.**

  We are subject to cyber-attacks. These cyber-attacks can vary in scope and intent from attacks with the objective of compromising our systems, networks and communications for economic gain to attacks with the objective of disrupting, disabling or otherwise compromising our operations. The attacks can encompass a wide range of methods and intent, including phishing attacks, illegitimate requests for payment, theft of intellectual property, theft of confidential or non-public information, installation of malware, installation of ransomware and theft of personal or business information. The breadth and scope of these attacks, as well as the techniques and sophistication used to conduct these attacks, have grown over time. We experienced a cybersecurity breach in January 2018 that resulted in a fraud loss of $144,200 where the probability of recovery of the loss is remote.

  A successful cyber-attack may target us directly, or it may be the result of a third party's inadequate care. In either scenario, we may suffer damage to our systems and data that could interrupt our operations, adversely impact our reputation and brand and expose us to increased risks of governmental investigation, litigation and other liability, any of which could adversely affect our business. Furthermore, responding to such an attack and mitigating the risk of future attacks could result in additional operating and capital costs in systems technology, personnel, monitoring and other investments.

  In addition, we are also subject to various risks associated with the collection, handling, storage and transmission of sensitive information. In the course of doing business, we collect employee, customer and other third-party data, including personally identifiable information and individual credit data, for various business purposes. These laws continue to develop and may be inconsistent from jurisdiction to jurisdiction. If we fail to comply with the

various applicable data collection and privacy laws, we could be exposed to fines, penalties, restrictions, litigation or other expenses, and our business could be adversely impacted.

Any breach, theft, loss, or fraudulent use of employee, third-party or company data, could adversely impact our reputation and expose us to risks of data loss, business disruption, governmental investigation, litigation and other liability, any of which could adversely affect our business. Significant capital investments and other expenditures could be required to remedy the problem and prevent future breaches, including costs associated with additional security technologies, personnel, experts and credit monitoring services for those whose data has been breached. Further, if we or our vendors experience significant data security breaches or fail to detect and appropriately respond to significant data security breaches, we could be exposed to government enforcement actions and private litigation." *Processa Pharmaceuticals, Inc., Form 10-K filed on March 6, 2020 (SIC 2834—Pharmaceutical Preparations)*

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 within the past five years (or such shorter period it may have been engaged in business) and to disclose material information from earlier periods necessary to understand the general development of its business. For more information on the Business section requirements, see Item 1. Description of Business under Form 10-K Drafting and Review — Overview of Major Disclosure Items. 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. Some examples of cybersecurity disclosures in the Business section are set forth below.

General Disclosure

- "As a provider of innovative network intelligence and security solutions for mobile and fixed service providers, we are 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 as an Israeli company. We are also aware of the 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.

  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 26, 2020 (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 26, 2020 (SIC 8093—Services—Specialty Outpatient Facilities, NEC)*

Disclosures for Financial Services Companies

- "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 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 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 27, 2020 (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.

  In late 2017, the SEC announced that it plans to issue guidelines governing the manner in which public companies report cybersecurity breaches to investors. 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 27, 2020 (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 27, 2020 (SIC 6211—Security Brokers, Dealers & Flotation Companies)*

Disclosures Relating to Actual or Known Cybersecurity Breaches

- "On July 29, 2019, we announced there was unauthorized access by an outside individual who 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'). The Cybersecurity Incident occurred on March 22 and 23, 2019. We believe the individual was able to exploit a specific configuration vulnerability in our infrastructure. We immediately fixed the configuration vulnerability that this individual exploited and verified there are no other instances in our environment. The person responsible was arrested by the Federal Bureau of Investigation on July 29, 2019, and federal prosecution of the responsible person has commenced. The U.S. Attorney's Office has stated they believe the data has been recovered and that there is no evidence the data was used for fraud or shared by this individual.

  This event affected approximately 100 million individuals in the United States and approximately 6 million in Canada. We believe no credit card account numbers or log-in credentials were compromised. The largest category of information accessed was information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019. This information included personal information that we routinely collect at the time we receive credit card applications, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income. In addition to credit card application data, the individual also obtained portions of credit card customer data, including customer status data (e.g., credit scores, credit limits, balances, payment history, contact information) and fragments of transaction data from a total of 23 days during 2016, 2017 and 2018. Approximately 120,000 Social Security numbers of our credit card customers and approximately 80,000 linked bank account numbers of our secured credit card customers were compromised in this incident. For our Canadian credit card customers, approximately 1 million Social Insurance Numbers were compromised in this incident.

  We provided required notification to affected individuals and made free credit monitoring and identity protection available. We retained a leading independent cybersecurity firm that confirmed we correctly identified and fixed the specific configuration vulnerability exploited in the Cybersecurity Incident.

  During the year, we incurred $72 million of incremental expenses related to the remediation of and response to the Cybersecurity Incident, largely driven by customer notifications, credit monitoring, technology costs, and professional support, offset by $34 million of insurance recoveries pursuant to our insurance coverage described below. These amounts were treated as adjusting items as it relates to our financial results ('Cyber Adjusting Items'). We expect to be at the low end of the $100 million to $150 million range previously disclosed for the total amount of Cyber Adjusting Items and expect that some of these costs will extend beyond 2019.

  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. We continue to expect that a significant portion of the Cyber Adjusting Items will be covered by insurance. Insurance reimbursements will also be treated as adjusting items, and the timing of recognizing insurance reimbursements may differ from the timing of recognizing the associated expenses.

  We continue to invest significantly in cybersecurity and expect to make additional investments as we continue to assess our cybersecurity program. These estimated investments are in addition to the estimated Cyber Adjusting Items, and we expect to absorb them within our existing operating efficiency ratio guidance.

  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 negatively impact our strategy or our long-term financial health. For more information, see 'Note 18-Commitments, Contingencies, Guarantees and Others.'

  Our reported results, excluding adjusting items, including the Cyber Adjusting Items, and our existing operating efficiency ratio guidance, represent non-GAAP measures which we believe help users of our financial information understand the impact of these adjusting items on our reported results as well as provide an alternate measurement of our operating performance." *Capital One Financial Corporation, Form 10-K filed on February 20, 2020 (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. We continue to cooperate with law enforcement in connection with the criminal investigation into the actors responsible for the 2017 cybersecurity incident. 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 20, 2020 (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. In addition, 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 28, 2020 (SIC 8071—Services—Medical Laboratories)*

Cybersecurity Disclosures in the MD&A Section

Item 303(a) (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 management believes to be important to, or that will likely have a material impact on, the company's business, financial position, or results of operations. For further information on the MD&A section, see Management's Discussion and Analysis of Financial Condition and Results of Operations 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. Some examples of cybersecurity breach disclosures in the MD&A section of periodic reports are set forth below.

General Disclosure

- "The Company is dependent upon the capacity, reliability and security of our information technology (IT) systems for our manufacturing, sales, financial and administrative functions. We also face the challenge of supporting our IT systems and implementing upgrades when necessary, including the prompt detection and remediation of any cybersecurity breaches.

  Our IT systems' security measures are focused on the prevention, detection and remediation of damage from computer viruses, natural disaster, unauthorized access, cyber-attack and other similar disruptions. However, our IT systems remain vulnerable to intrusion and damage despite our implementation of security measures that we feel protect our IT systems. To date, we are not aware of any cybersecurity breaches that have negatively impacted our manufacturing operations, sales or financial and administrative functions or that resulted in the compromise of personal information of our employees, customers or suppliers. Should we learn of such a breach, the Company would promptly notify the SEC by filing a Form 8-K and notify all insiders that the purchase or sale of the Company's stock is forbidden until such information has been given adequate time to become available to the trading public." *Continental Materials Corporation, Form 10-K filed on March 23, 2020 (SIC 3270—Concrete, Gypsum & Plaster Products)*

Cybersecurity Risk Management Disclosure

- "We continually monitor and address cybersecurity risk. We have taken action to ensure data privacy and security for our customers on our e-commerce platform as well as require regular cybersecurity training for our employees.

  New employees are required to complete cybersecurity training upon hire and all other employees are required to complete cybersecurity training on an annual basis. The cybersecurity training topics include GDPR requirements, email security, strong password creation and usage and phishing. The phishing training has provided tangible results. Our phishing click rate has been steady between 8.4% and 8.7%, which is industry leading and well below the industry average of 13%.

  Our 2018 acquisition activity created many disparate e-commerce shopping experiences. In 2019, we introduced a single consolidated e-commerce platform supporting cross brand shopping. The consolidated e-commerce platform bolstered the following cybersecurity defenses by: providing a modern, supported platform by Magento; consolidating to a single codebase to support and secure compared to three different code bases under the previous sites; using an application firewall built into the product to reduce ZAGG's exposure to Distributed Denial-of-Service (DDoS) attacks; and deploying software updates managed by the Magento support staff.

  In 2020, we will continue to review password policies across the organization. Our IT department will begin looking into and testing password-less policies by using FIDO2 keys and Authenticator apps to completely remove the need for employee and service passwords. This will further reduce any exposure to phishing attacks against ZAGG personnel. We recently implemented a SIEM platform, which has been instrumental in consolidating systems events and security logs. This allows for incident hunting and better security analytics to be leveraged by the security team." *ZAGG Inc., Form 10-K filed on March 16, 2020 (SIC 5900—Retail—Miscellaneous Retail)*

Disclosures Relating to Actual or Known Cybersecurity Breaches

- "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, with a remaining insurance receivable of $50 at December 31, 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 11, 2020 (SIC 6021—National Commercial Banks)*

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

  To date, we have not seen a meaningful impact on demand as a result of the Data Security Incident.

  In July 2019, the ICO issued a formal notice of intent under the U.K. Data Protection Act 2018 proposing a fine in the amount of £99 million against the Company in relation to the Data Security Incident (the 'Proposed ICO Fine'). We mutually agreed with the ICO to an extension of the regulatory process until June 1, 2020, and the ICO proceeding is ongoing. In the 2019 second quarter, we recorded an accrual in the full amount of the Proposed ICO Fine for this loss contingency, and in the 2019 fourth quarter, we reduced the accrual to $65 million based on the ongoing proceeding. See Note 7 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 increased for our current policy period, and the cost of such insurance could continue to increase in future years. 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 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 7 for information related to expenses incurred in 2018 and 2019, insurance recoveries, and legal proceedings and governmental investigations related to the Data Security Incident." *Marriott International, Inc., Form 10-K filed on February 27, 2020 (SIC 7011—Hotels & Motels)*

- "In August 2019, we experienced a network security incident caused by malware that prevented access to several of our information technology systems and data. Following the discovery of the incident, we promptly took actions to isolate and shut down affected systems based on our existing protocols. We implemented our business continuity plan and undertook actions to recover the affected systems. We believe we were successfully able to restore the operation of the systems without loss of business data. Based on the nature of the network security incident, the impact on our information technology systems and the results of the forensic IT analysis, we do not believe confidential customer, employee, or company data was lost or disclosed. Our stores remained open and operating throughout the incident, but were utilizing manual back-up processes for approximately six days which we believe had an adverse impact on sales. We maintain cyber-security and other insurance and have been working collaboratively with our carriers. As of December 31, 2019, we estimate the equipment replaced and costs associated with the incident to date to be approximately $3.7 million. During 2019, we received an initial recovery from insurance in excess of $2 million, capitalized new equipment, and recorded approximately $0.8 million as a receivable related to further anticipated recovery. The receivable is recorded in 'Other Current Assets' on the Consolidated Balance Sheets and does not include any potential business interruption recovery or involuntary gains related to the incident." *Lumber Liquidators Holdings, Inc., Form 10-K filed on February 25, 2020 (SIC 5211—Retail—Lumber & Other Building Materials Dealers)*

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

- "On December 15, 2019, and ending on December 18, 2019, Pike was impacted by a Ransomware attack. At no time did Pike lose the ability to provide critical services to its customers or effectively respond to system emergencies. Pike lost the ability to utilize internal accounting system and their customer information systems. The Company believes that no customer information or employee data was compromised or stolen; this assumption will be confirmed once forensics have been completed. The Company did not pay any ransom and has had no communications with the perpetrators of the event. This event did not impact Corning Gas.

  On December 24, 2019, the Gas Company was the victim of a ransomware attack which rendered its accounting system and customer service system inoperable from December 24, 2019, through December 28, 2019. The restoration of the systems was completed by in-house IT Staff as well as two IT firms that were under contract with the Company. The Company did not lose the ability to provide critical services to its customers. The Company did not lose the ability to effectively respond to system emergencies. The Company believes that no data was compromised as a result of this ransomware attack. Prior to this event the Company had engaged KnowBe4 to provide employee cyber security training. The Company had also contracted with AXIO to complete a Cyber Security Capability Maturity Model Evaluation 'C2M2' and IT & Cyber Security Risk Management Program. The C2M2 evaluation was completed prior to the event. The IT&CS risk management program is still in development and the Company continues to utilize the expertise of KnowBe4 and AXIO. After the attack the Company has revised its VPN policies, implemented new password protocols and added two factor authentications requirements for all system users. The Company has also added greater visibility to ongoing patching and backup procedures. The Company also contracted for endpoint monitoring and cyber security services with Kroll, a division of Duff & Phelps." *Corning Natural Gas Holding Corporation, Form 10-Q filed on February 13, 2020 (SIC 4923—Natural Gas Transmission & Distribution)*

Disclosure regarding Ongoing Litigation Related to Cybersecurity Breaches

- "In February 2016, the Company reported unusual payment card activity affecting some franchise owned restaurants and that malware had been discovered on certain systems. In June 2016, the Company reported that an additional malware variant had been identified and disabled. In July 2016, the Company, on behalf of affected franchise locations, provided information about specific restaurant locations that may have been impacted by these attacks, all of which were located in the United States, along with support for customers who may have been affected by the malware.

  During 2019, the Company entered into settlement agreements to resolve a consumer class action and a financial institutions class action related to the cybersecurity incidents. The consumer class action settlement was approved by the court in February 2019 and the financial institutions class action settlement was approved by the court in November 2019. Both matters are now considered fully paid and closed. Under the terms of the settlement agreement for the financial institutions class action, the Company and its franchisees received a full release of all claims that have or could have been brought by the financial institutions, and the financial institutions received $50.0 million, inclusive of attorneys' fees and costs. After exhaustion of applicable insurance receivables, the Company made a payment of $24.7 million of this amount in January 2020. During 2018, the Company recorded a liability of $50.0 million and insurance receivables of $22.5 million for the financial institutions case. During 2019, as a result of cost savings related to the settlement of the consumer class action, the Company adjusted its insurance receivables for the financial institutions case to approximately $25.0 million." *The Wendy's Company, Form 10-K filed on February 26, 2020 (SIC 5810— Retail— Eating & Drinking Places)*

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 be helpful 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 ascertain if 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 if 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 is expected to provide additional cybersecurity disclosures to underscore its special circumstances, such as having a strong e-commerce presence, outsourcing business functions, handling its own business and personnel data, having a platform for online financial transactions, collecting and storing health-related records of its clientele, having public safety concerns due to the nature of the industry the company is in, or having an insurance covering 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 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., 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 Disclosure.
- **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 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 Go, Associate, Mayer Brown LLP

Gonzalo D.V. Go III is an associate in Mayer Brown's Corporate & Securities practice. He advises issuers, investment banks and sponsors in public and private offerings of equity and debt securities, including initial public offerings; follow-on offerings; investment grade, high-yield debt offerings; covered bonds; real estate investment trusts and structured products linked to equities, commodities, interest rates, currencies and other underlying assets.

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) the legal director of 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 a tier-one 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.