Market Trends 2018/19: Cybersecurity Related Disclosures

A Lexis Practice Advisor® Practice Note by Mingli Wu and Hanwen Zhang, Mayer Brown LLP

Mingli Wu
Mayer Brown LLP

Hanwen Zhang
Mayer Brown LLP

This market trends article identifies comprehensive disclosures related to cybersecurity risks, including discussions about the potential reputational, financial, or operational harm resulting from cybersecurity breaches; the potential associated litigation or regulatory costs; and their policies and procedures addressing cybersecurity incidents, and concludes with practical advice on preparing the required disclosures regarding cybersecurity risks and incidents. The company name, its industry, and the type of filing are also provided in each sample disclosure for reference.

On October 16, 2018, the Securities and Exchange Commission (SEC) released a report of investigation 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, in his speech, the SEC Chairman Jay Clayton 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 (2018 guidance) issued earlier in 2018.

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.

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). To date, most of the disclosures related to cybersecurity risks and incidents tend to be quite general in nature. On the other hand, there are a growing number of companies that provide disclosures that are more comprehensive and particularized, with discussions about the potential reputational, financial, or operational harm resulting from cybersecurity breaches, the potential associated litigation or regulatory costs, and their policies and procedures addressing cybersecurity 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.

Risk Factor Disclosures

Item 503(c) (17 C.F.R. § 229.503) of Regulation S-K requires that a company describe the material risks that impact the company's business, results of operations, and future prospects, as well as material risks that make an investment in the offered securities speculative or risky, in the case of an offering document. 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 Glossaries in Prospectuses and Annual Reports — Background. 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 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 cybersecurity incidents become known, companies typically disclose the incidents together with remedial actions, estimated losses, and other consequences, such as litigation and regulatory action associated with the incidents. For a further discussion on cybersecurity disclosure, see Media & Entertainment Industry Practice Guide — Regulatory Trends. Set forth below are some examples of cybersecurity disclosures in the Risk Factor section.

General Disclosure on Cybersecurity Risks

- **"Operational risks, including cybersecurity risks, may disrupt our businesses, result in losses or limit our growth."**

  In addition, our systems face ongoing cybersecurity threats and attacks. Attacks on our systems could involve, and in some instances have in the past involved, attempts intended to obtain unauthorized access to our proprietary information, destroy data or disable, degrade or sabotage our systems, including through the introduction of computer viruses, 'phishing' attempts and other forms of social engineering. Cyberattacks and other security threats could originate from a wide variety of sources, including cyber criminals, nation state hackers, hacktivists and other outside parties. There has been an increase in the frequency and sophistication of the cyber and security threats we face, with attacks ranging from those common to businesses generally to those that are more advanced and persistent, which may target us because, as an alternative asset management firm, we hold a significant amount of confidential and sensitive information about our investors, our portfolio companies and potential investments. As a result, we may face a heightened risk of a security breach or disruption with respect to this information. If successful, these types of attacks on our network or other systems could have a material adverse effect on our business and results of operations, due to, among other things, the loss of investor or proprietary data, interruptions or delays in our business and damage to our reputation. There can be no assurance that measures we take to ensure the integrity of our systems will provide protection, especially because cyberattack techniques used change frequently or are not recognized until successful. If our systems are compromised, do not operate properly or are disabled, or we fail to provide the appropriate regulatory or other notifications in a timely manner, we could suffer financial loss, a disruption of our businesses, liability to our investment funds and fund investors, regulatory intervention or reputational damage.

  In addition, we operate in businesses that are highly dependent on information systems and technology. The costs related to cyber or other security threats or disruptions may not be fully insured or indemnified by other means. In addition, cybersecurity has become a top priority for regulators around the world. Many jurisdictions in which we operate have laws and regulations relating to data privacy, cybersecurity and protection of personal information, including the General

Data Protection Regulation in the European Union that went into effect in May 2018. Some jurisdictions have also enacted laws requiring companies to notify individuals of data security breaches involving certain types of personal data. Breaches in security could potentially jeopardize our, our employees' or our fund investors' or counterparties' confidential and other information processed and stored in, and transmitted through, our computer systems and networks, or otherwise cause interruptions or malfunctions in our, our employees', our fund investors', our counterparties' or third parties' operations, which could result in significant losses, increased costs, disruption of our business, liability to our fund investors and other counterparties, regulatory intervention or reputational damage. Furthermore, if we fail to comply with the relevant laws and regulations, it could result in regulatory investigations and penalties, which could lead to negative publicity and may cause our fund investors and clients to lose confidence in the effectiveness of our security measures." Blackstone Group L.P., 10-K filed March 1, 2019 (SIC 6282—Investment Advice)

Disclosures for Companies That Have a Strong E-commerce Presence

- **"Our business is subject to online security risks, including security breaches and cyber attacks."**

  Our businesses involve the storage and transmission of users' personal financial information . . . The techniques used to obtain unauthorized access, disable, or degrade service, or sabotage systems, change frequently, may be difficult to detect for a long time, and often are not recognized until launched against a target. Certain efforts may be state sponsored and supported by significant financial and technological resources and therefore may be even more difficult to detect. As a result, we may be unable to anticipate these techniques or to implement adequate preventative measures. Unauthorized parties may also attempt to gain access to our systems or facilities through various means, including hacking into our systems or facilities, fraud, trickery or other means of deceiving our employees, contractors and temporary staff. A party that is able to circumvent our security measures could misappropriate our or our users' personal information, cause interruption or degradations in our operations, damage our computers or those of our users, or otherwise damage our reputation . . . Our information technology and infrastructure may be vulnerable to cyberattacks or security incidents and third parties may be able to access our users' proprietary information and payment card data that are stored on or accessible through our systems. Any security breach at a company providing services to us or our users could have similar effects.

  We may also need to expend significant additional resources to protect against security breaches or to redress problems caused by breaches. These issues are likely to become more difficult and costly as we expand the number of markets where we operate. Additionally, our insurance policies carry low coverage limits, which may not be adequate to reimburse us for losses caused by security breaches and we may not be able to fully collect, if at all, under these insurance policies." eBay Inc., Form 10-K filed January 30, 2019 (SIC 7389 Services—Business Services)

- **"The Online Nature of Our Company's Operations Exposes the Company to Additional Cyber security Risks."**

  The Company is heavily engaged in Blockchain mining and the development of a planned digital currency exchange, all of which are inherently dependent on and exposed to the internet. Accordingly, hacking and unauthorized access to the Company's internal systems poses a substantial threat. The Company, through its platform, RiotX, anticipates the use of multiple digital wallets to secure customer assets. These digital wallets will have policy controls that require multiple approvals, spending limits and whitelists for transactions. The Company's digital wallet provider is anticipated to also support multi-signature, three-key management which removes any single point of failure and advanced security configurations ensure that assets are secure as they move in and out of the digital wallet. By employing multiple independent digital wallets, the Company plans to implement several fail-safes against a potential breach, such as; assets in a given wallet are completely segregated from assets in another wallet, except for access by the authorized user(s). Furthermore, the Company is presently in discussions with third-party providers for custodial services of customer assets exchanged on its planned RiotX digital currency exchange. The Company will have a qualified third-party custodian to secure customer digital assets in keeping with industry rules and best practices. No system is totally secure and even the most sophisticated systems face the risk of unauthorized access and asset seizure. Digital currency keys which provide access to digital wallets and the digital currencies contained therein, are the most likely and vital assets

for an attack, and the Company has taken or plans to take appropriate action to abrogate such risk as much as possible. An unauthorized user with access to the Company's digital keys could conceivably transfer all of the Company's digital currency assets and the Company would have limited ability to recover such stolen assets. To protect against this risk, the Company intends to employ a 95% 'cold storage' policy for all digital currencies exchanged on RiotX. Cold Storage assets are air-gapped to the internet providing an additional layer of security, meaning that a potential unauthorized online penetration of RiotX or its vendors would not be able to impact the offline digital currency keys. Despite these safeguards, there is still risk of loss or theft of digital currencies or access to the planned exchange due to the prevalence of ransomware, DDOS, and other malware/ hacking attacks which pervade the internet. A successful hacking operation of the Company or its planned exchange could result in substantial impacts on the financial and business operations of the Company." Riot Blockchain, Inc., Form 10-Q/A filed March 6, 2019 (SIC 2835— In Vitro & In Vivo Diagnostic substances)

- **"Any failure by us to protect the confidential information of our customers and employees, and our networks against security breaches and the risks associated with credit card fraud could damage our reputation and brands and substantially harm our business and results of operations."**

  A significant prerequisite to e-commerce and communications is the secure transmission of confidential information over public networks . . . Even though we do not store customer credit cards on our computer system and use third-party systems to clear transactions, in case of an outage to a third-party system, we will temporarily store and bill our customers' credit card accounts directly; orders are then shipped to a customer's address and customers log on using their email address. We rely on encryption and authentication technologies licensed from third parties to affect the secure transmission of confidential information, including credit card numbers . . . In addition, any party who is able to illicitly obtain a user's password could access the user's transaction data, personal information or stored images. In addition to these threats, the security, integrity, and availability of our customers' and employees' data, including student photos, could be compromised by employee negligence, error or malfeasance, and technology defects. For example, due to the current status of Lifetouch's customer contact processes, there is risk of providing photo access to the wrong customer, which could lead to loss of business with school districts and lead to brand reputation damage.

  Our expanded use of cloud-based services could also increase the risk of security breaches as cyberattacks on cloud environments are increasing to almost the same level as attacks on traditional information technology systems. For example, in 2014, we experienced a cyberattack on our Tiny Prints, Treat and Wedding Paper Divas websites, which may have exposed the email addresses and encrypted passwords used by our customers to login to their accounts. We encrypt customer credit and debit card information, and we have no evidence that such information was compromised; however, any compromise of our security could damage our reputation and brands and expose us to a risk of loss or litigation and potential liability, which would substantially harm our business and results of operations. In addition, anyone who can circumvent our security measures could misappropriate proprietary information or cause interruptions in our operations. We may need to devote significant resources to protect against security breaches or to address problems caused by breaches. Additionally, in 2018, we discovered that there had been unauthorized access to an internal testing environment, which could have resulted in exposure of employee confidential data. Although we discovered no evidence to indicate exposure of this data, we cannot determine that it did not occur; while we have taken remediation and precautionary measures to prevent this type of situation from occurring again, we cannot guarantee that these measures [sic] will be effective." Shutterfly, Inc., Form 10-K filed March 1, 2019 (SIC 7384 Services— Photofinishing Laboratories)

Disclosures on Intersection of Cybersecurity and Data Privacy

- **"We are subject to cybersecurity risks that could negatively impact our business operations."**

  We are dependent upon our information technology platform, including our processing systems, data and electronic transmissions in our business operations [. . .] The NAIC has adopted an Insurance Data Security Model Law, which, when adopted by the states will require insurers, insurance producers and other entities required to be licensed under state insurance laws to comply with certain requirements under state insurance laws, such as developing and maintaining a written information security program, conducting risk assessments and overseeing the

data security practices of third-party vendors. In addition, certain state insurance regulators are developing or have developed regulations that may impose regulatory requirements relating to cybersecurity on insurance and reinsurance companies (potentially including insurance and reinsurance companies that are not domiciled, but are licensed, in the relevant state). For example, the New York State Department of Financial Services has adopted a regulation pertaining to cybersecurity for all banking and insurance entities under its jurisdiction, effective as of March 1, 2017, which applies to us. We cannot predict the impact these laws and regulations will have on our business, financial condition or results of operations, but our insurance and reinsurance companies could incur additional costs resulting from compliance with such laws and regulations." Everest Reinsurance Holdings Inc. Form 10-K filed April 1, 2019 (SIC 6331—Fire, Marine & Casualty Insurance)

- **"We are exposed to risks related to cybersecurity threats and general information security incidents which may also expose us to liability under data protection laws including the GDPR."**

  Cybersecurity incidents may result in business disruption, the misappropriation, corruption or loss of confidential information (including personally identifiable information) and critical data (ours or that of third parties), reputational damage, litigation with third parties, regulatory fines, diminution in the value of our investment in research and development and data privacy issues and increased information security protection and remediation costs. As these cybersecurity threats, and government and regulatory oversight of associated risks continue to evolve, we may be required to expend additional resources to remediate, enhance or expand upon the cybersecurity protection and security measures we currently maintain. For example, we are subject to the European Union's General Data Protection Regulation (GDPR), which became enforceable from May 25, 2018. The GDPR introduced a number of new obligations for subject companies resulting in the need to continue dedicating financial resources and management time to GDPR compliance. While we have taken steps to ensure compliance with the GDPR, there can be no assurance that the measures we have taken will be successful in preventing an incident, including a cybersecurity incident or other data breach, which results in a breach of the GDPR. Individuals who have suffered damage as a result of a subject company's noncompliance with the GDPR also have the right to seek compensation from such a company. Future cybersecurity breaches, general information security incidents, further increases in data protection costs or failure to comply with relevant legal obligations regarding protection of data could therefore have a material adverse effect on our results of operations, financial position and cash flows." MYOS RENS Technology Inc. Form 10-K filed March 27, 2019 (SIC 2834—Pharmaceutical Preparations)

Cybersecurity Disclosures Relating to Actual or Known Breaches and Litigation in Connection with the Breaches

- **"Security breaches and improper access to or disclosure of our data or user data, or other hacking and phishing attacks on our systems, could harm our reputation and adversely affect our business."**

  For example, in September 2018, we announced our discovery of a third-party cyberattack that exploited a vulnerability in Facebook's code to steal user access tokens, which were then used to access certain profile information from approximately 29 million user accounts on Facebook. While we took steps to remediate the attack, including fixing the vulnerability, resetting user access tokens and notifying affected users, we may discover and announce additional developments, which could further erode confidence in our brand. In addition, the events surrounding this cyberattack became the subject of Irish Data Protection Commission, U.S. Federal Trade Commission and other government inquiries in the United States, Europe, and other jurisdictions. Any such inquiries could subject us to substantial fines and costs, require us to change our business practices, divert resources and the attention of management from our business, or adversely affect our business.

  [. . .] we are currently the subject of multiple putative class action suits in connection with [. . .] a third-party cyberattack that exploited a vulnerability in Facebook's code to steal user access tokens and access certain profile information from user accounts on Facebook." Facebook Inc., Form 10-K filed January 31, 2019 (SIC 7389—Services—Computer Programming, Data Processing, Etc.)

- **"We face significant cyber and data security risk that could result in the disclosure of confidential information, adversely affect our business or reputation and expose us to significant liabilities."**

  In July 2017, we incurred a loss of approximately $172 thousand due to fraudulent wire transactions. These fraudulent wire transactions were the result of an email

phishing scheme that targeted various employees of the Bank and led to an internal email compromise, affording the perpetrators access to personal information of a number of the Bank's customers. We took immediate action to contain and eradicate the email compromise, including the implementation of control enhancements to prevent a similar situation from occurring again. We believe this was an isolated event and do not believe our technology systems have been compromised. While we have not experienced any material losses relating to cyberattacks or other information security breaches such as the one that occurred in July 2017, we have been the subject of a successful hacking and cyberattack and there can be no assurance that we will not suffer additional losses in the future related to this event or others.

The occurrence of any cyberattack or information security breach, such as the one that occurred in July 2017, could result in material adverse consequences to us including damage to our reputation and the loss of customers. We also could face litigation or additional regulatory scrutiny. Litigation or regulatory actions in turn could lead to significant liability or other sanctions, including fines and penalties or reimbursement of customers adversely affected by this security breach. Even if we do not suffer any material adverse consequences as a result of the event that occurred in July 2017 or as a result of other future events, successful attacks or systems failures at the Bank or at other financial institutions could lead to a general loss of customer confidence in financial institutions including the Bank.

Our ability to mitigate the adverse consequences of occurrences (such as the one in July 2017) is in part dependent on the quality of our information security procedures and contracts and our ability to anticipate the timing and nature of any such event that occurs. In recent years, we have incurred significant expense towards improving the reliability of our systems and their security from attack. Nonetheless, there remains the risk that we may be materially harmed by this cyberattack and information security breach or others in the future. Methods used to attack information systems change frequently (with generally increasing sophistication), often are not recognized until launched against a target, may be supported by foreign governments or other well-financed entities, and may originate from less regulated and remote areas around the world. As a result, we may be unable to address these methods in advance of attacks, including by implementing adequate preventive measures. If such an attack or breach does occur again, we might not be able to fix it timely or adequately. To the extent that such an attack or breach relates to products or services provided by others, we seek to engage in due diligence and monitoring to limit the risk. In addition, as the regulatory environment related to information security, data collection and use, and privacy becomes increasingly rigorous, with new and constantly changing requirements applicable to our business, compliance with those requirements could also result in additional costs." Southern National Bancorp of Virginia, Inc. 10-K filed March 15, 2019 (SIC 6022—State Commercial Banks)

- **"Security breaches like the 2017 cybersecurity incident and other disruptions to our information technology infrastructure could compromise Company, consumer and customer information, interfere with our operations, cause us to incur significant costs for remediation and enhancement of our IT systems and expose us to legal liability, all of which could have a substantial negative impact on our business and reputation."**

  [. . .] In 2017, we were the target of a cybersecurity attack that involved the theft of certain personally identifiable information of approximately 145.5 million U.S. consumers, approximately 19,000 Canadian consumers and approximately 860,000 UK consumers. In addition, we identified approximately 2.4 million U.S. consumers whose name and partial driver's license information were stolen in the attack. While the forensic analysis of the 2017 cybersecurity incident is complete, it is possible that further analysis will identify additional consumers affected or additional types of data accessed, which could result in additional notifications and negative publicity.

  Following the 2017 cybersecurity incident, we began undertaking significant remediation efforts and other steps to enhance our data security infrastructure which are ongoing. In connection with these efforts, we have incurred significant costs and expect to incur additional significant costs as we continue to enhance our data security infrastructure and take further steps to prevent unauthorized access to our systems and the data we maintain. Despite these efforts, we cannot assure you that all potential causes of this incident have been identified and remediated and that similar cyber incidents will not occur in the future." Equifax Inc., Form 10-K filed February 21, 2019 (SIC 7320 Services—Consumer Credit Reporting, Collection Agencies)

- **"The government investigations and litigation resulting from the 2017 cybersecurity incident will continue to adversely impact our business and results of operations."**

  As a result of the 2017 cybersecurity incident, we are currently a party to a consolidated multidistrict consumer class action lawsuit and a consolidated multidistrict financial institution class action lawsuit, as well as a consolidated securities class action lawsuit, shareholder derivative litigation and other lawsuits and claims arising out of the 2017 cybersecurity incident seeking monetary damages or other relief. A number of U.S. federal, state, local and foreign governmental officials and agencies, including Congressional committees, the FTC, the CFPB, the SEC, the U.S. Department of Justice and state attorneys general offices in the U.S., the FCA in the UK and the Office of the Privacy Commissioner in Canada, continue to investigate events related to the 2017 cybersecurity incident, including how it occurred, the consequences thereof and our response thereto . . . In addition, other lawsuits, investigations and reports related to the 2017 cybersecurity incident may be filed, commenced or issued. The claims and investigations have resulted in the incurrence of significant external and internal legal costs and expenses and reputational damage to our business and are expected to continue throughout 2019 and beyond. The resolution of these matters may result in damages, costs, fines or penalties substantially in excess of our insurance coverage, which, depending on the amount, could have a material adverse effect on our liquidity or compliance with our credit agreements. If such damages, costs, fines or penalties were great enough that we could not pay them through funds generated from operating activities and/or cause a default under our revolving credit facility, we may be forced to renegotiate or obtain a waiver under our revolving credit facility and/or seek additional debt or equity financing. Such renegotiation or financing may not be available on acceptable terms, or at all. In these circumstances, if we were unable to obtain sufficient financing, we may not be able to meet our obligations as they come due. The outcome of such claims and investigations could also adversely affect or cause us to change how we operate our business. Various governmental agencies investigating the 2017 cybersecurity incident are seeking to impose injunctive relief, consent decrees, and civil penalties, which could, among other things, impact our ability to collect and use consumer information, materially increase our data security costs, reduce available resources to invest in technology and innovation and/or otherwise require us to alter how we operate our business, and put us at a competitive disadvantage." Equifax Inc., Form 10-K filed February 21, 2019 (SIC 7320—Services—Consumer Credit Reporting, Collection Agencies)

- **"If our efforts to protect the security of information about our guests, team members, vendors and other third parties are unsuccessful, we may face additional costly government enforcement actions and private litigation, and our sales and reputation 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 sales, reputation and results of operations. The legal and regulatory environment regarding information security, cybersecurity, and privacy is increasingly demanding and has enhanced requirements for handling personal data. Complying with new data protection requirements 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 Corp., Form 10-K filed March 13, 2019 (SIC 5331—Retail—Variety Stores)

Cybersecurity Breach Disclosures Contained 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 a shorter period in which it may have engaged in

business, including the information from earlier periods that is material. For more information on the Business section requirements, see Form 10-K Drafting and Review — Overview of Major Items of Disclosure. In their Business sections, a number of public companies disclosed that cybersecurity risks pose a threat to their intellectual property, patents, and trade secrets. Also, many public companies noted that most states have adopted data security breach laws and disclosed that compliance with these government regulations may be costly. These disclosures are mostly brief and do not discuss in detail the degree to which the company's business would be affected by cybersecurity incidents. Set forth below are some examples of cybersecurity breach risk disclosures in the Business sections of filings.

General Disclosure

- "We may rely, in some circumstances, on trade secrets to protect our technology. However, trade secrets can be difficult to protect. We seek to protect our proprietary technology and processes, in part, by confidentiality agreements and assignment of inventions agreements with our employees, consultants, scientific advisors and contractors. We also seek to preserve the integrity and confidentiality of our data and trade secrets by maintaining physical security of our premises and physical and electronic security of our information technology systems. While we have confidence in these individuals, organizations and systems, such agreements or security measures may be breached, and we may not have adequate remedies for any breach. In addition, our trade secrets may otherwise become known or be independently discovered by competitors or others." Can-Fite BioPharma Ltd., Form 20-F/A filed April 2, 2019 (SIC 2834—Pharmaceutical Preparations)
- "Although we have confidence in these individuals, organizations, and systems, agreements or security measures may be breached and we may not have adequate remedies for any breach. In addition, our trade secrets may otherwise become known or may be independently discovered by competitors. To the extent that our employees, contractors, consultants, collaborators, and advisors use intellectual property owned by others in their work for us, disputes may arise as to the rights in related or resulting know-how and inventions."NantHealth, Inc., Form 10-K filed April 1, 2019 (SIC 7374—services—Computer Processing & Data Preparation]

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 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." First Interstate Bancsystem, Inc., Form 10-K filed February 27, 2019 (SIC 6022—State Commercial Banks)

Cybersecurity Disclosures Relating to Actual or Known Breaches

- "As a financial institution holding company, NBI is subject to cybersecurity risks and has suffered two cybersecurity incidents. To manage and mitigate cybersecurity risk, the Company limits certain transactions and interactions with customers. The Company does not offer online account openings or loan originations, limits the dollar amount of online banking transfers to other banks, does not permit customers to submit address changes or wire requests through online banking, requires a special vetting process for commercial customers who wish to originate ACH transfers, and limits certain functionalities of mobile banking. The Company also requires assurances from key vendors regarding their cybersecurity. While these measures reduce the likelihood and scope of the risk of further cybersecurity breaches, in light of the evolving sophistication of system intruders, the risk of such breaches continues to exist. We maintain insurance for these risks but insurance policies are subject to exceptions, exclusions and terms whose applications have not been widely interpreted in litigation. Accordingly, insurance can provide less than complete protection

against the losses that result from cybersecurity breaches and pursuing recovery from insurers can result in significant expense. In addition, some risks such as reputational damage and loss of customer goodwill, which can result from cybersecurity breaches cannot be insured against." National Bankshares, Inc., Form 10-K filed March 13, 2019 (SIC 6021—National Commercial Banks)

Disclosure regarding Ongoing Litigation Related to Cybersecurity Breaches

- "The Company is involved in litigation and claims incidental to our current and prior businesses. We provide accruals for such litigation and claims when payment is probable and reasonably estimable. We believe we have adequate accruals for continuing operations for all of our legal and environmental matters, including the accrual that we recorded for the legal proceedings related to a cybersecurity incident as described in Note 23 of the Financial Statements and Supplementary Data contained in Item 8 herein. See Note 11 of the Financial Statements and supplementary Data contained in Item 8 herein for further information on the accrual. We cannot estimate the aggregate possible range of loss for various reasons, including, but not limited to, many proceedings being in preliminary stages, with various motions either yet to be submitted or pending, discovery yet to occur and/or significant factual matters unresolved. In addition, most cases seek an indeterminate amount of damages and many involve multiple parties. Predicting the outcomes of settlement discussions or judicial or arbitral decisions is thus inherently difficult and future developments could cause these actions or claims, individually or in aggregate, to have a material adverse effect on the Company's financial condition, results of operations or cash flows for a particular reporting period." The Wendy's Company, Form 10-K filed February 27, 2019 (SIC 6021—5810—Retail—Eating & Drinking Places)
- "Cyberattack Class Actions Litigation. In January 2014, three class actions relating to a cyberattack on our computer systems in 2013 were filed and later voluntarily dismissed by the plaintiffs between February and April 2014. The plaintiffs had alleged negligence and other claims in connection with their purchases by payment cards and sought monetary and injunctive relief. Three additional putative class actions relating to the cyberattack were filed in March and April 2014, also alleging negligence and other claims in connection with plaintiffs' purchases by payment cards. Two of the cases were voluntarily dismissed. The third case, Hilary Remijas v. The Neiman Marcus Group, LLC, was filed on March 12, 2014 in the U.S. District Court for the Northern District of Illinois. On June 2, 2014, an amended complaint in the Remijas case was filed, which added three plaintiffs (Debbie Farnoush and Joanne Kao, California residents; and Melissa Frank, a New York resident) and asserted claims for negligence, implied contract, unjust enrichment, violation of various consumer protection statutes, invasion of privacy and violation of state data breach laws. The Company moved to dismiss the Remijas amended complaint, and the court granted the Company's motion on the grounds that the plaintiffs lacked standing due to their failure to demonstrate an actionable injury. Plaintiffs appealed the district court's order dismissing the case to the Seventh Circuit Court of Appeals, and the Seventh Circuit Court of Appeals reversed the district court's ruling, remanding the case back to the district court. The Company filed a petition for rehearing en banc, which the Seventh Circuit Court of Appeals denied. The Company filed a motion for dismissal on other grounds, which the court denied. The parties jointly requested, and the court granted, an extension of time for filing a responsive pleading, which was due on December 28, 2016. On February 9, 2017, the court denied the parties' request for another extension of time, dismissed the case without prejudice, and stated that plaintiffs could file a motion to reinstate. On March 8, 2017, plaintiffs filed a motion to reinstate, which the court granted on March 16, 2017. On March 17, 2017, plaintiffs filed a motion seeking preliminary approval of a class action settlement resolving this action, which the court granted on June 21, 2017. On August 21, 2017, plaintiffs moved for final approval of the proposed settlement. In September 2017, purported settlement class members filed two objections to the settlement, and plaintiffs and the Company filed responses to the objections on October 19, 2017. At the fairness hearing on October 26, 2017, the Court ordered supplemental briefing on the objections. Objectors filed a supplemental brief in support of their objections on November 9, 2017, and plaintiffs and the Company filed their supplemental responses to the objections on November 21, 2017. On January 16, 2018, an order was issued by the District Court reassigning the case to Judge Sharon Johnson Coleman due to the prior judge's retirement. On September 17, 2018, Judge Coleman denied final approval of the proposed settlement and decertified the settlement class. Judge Coleman has set a status conference for this matter for April 12, 2019. At this point, we are unable to predict the developments in, outcome of or other consequences related to this matter.

In addition to class actions litigation, payment card companies and associations may require us to reimburse them for unauthorized card charges and costs to replace cards and may also impose fines or penalties in connection with the security incident, and enforcement authorities may also impose fines or seek other remedies against us. We have also incurred other costs associated with this security incident, including legal fees, investigative fees, costs of communications with customers and credit monitoring services provided to our customers. We expect to continue to incur costs associated with maintaining appropriate security measures and otherwise complying with our obligations. We will continue to evaluate these matters based on subsequent events, new information and future circumstances." Neiman Marcus Group LTD LLC Form 10-Q filed March 12, 2019 (SIC 5311—Retail—Department Stores)

Cybersecurity Breach 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 or factors that management believes to be important to, or that affect, the company's 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. A small number of 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

- "Data security and integrity are critically important to our business, and breaches of security, unauthorized access to or disclosure of confidential information, disruption, including distributed denial of service attacks or the perception that confidential information is not secure, could result in a material loss of business, substantial legal liability or significant harm to our reputation." Red Violet, Inc. Form 10-K filed March 7, 2019 (SIC 7372—Services—Prepackaged Software)

Cybersecurity Risk Management Disclosures

- "Our internal computer systems, or those that are expected to be used by our clinical investigators, clinical research organizations or other contractors or consultants, may fail or suffer security breaches, which could result in a material disruption of development programs for our product candidates.

  We rely on information technology systems to keep financial records, maintain laboratory and corporate records, communicate with staff and external parties and operate other critical functions. Any significant degradation or failure of these computer systems could cause us to inaccurately calculate or lose data. Despite the implementation of security measures, these internal computer systems and those used by our clinical investigators, clinical research organizations, and other contractors and consultants are vulnerable to damage from computer viruses, unauthorized access, natural disasters, terrorism, war, and telecommunication and electrical failures. The techniques that could be used by criminal elements or foreign governments to attack these computer systems are sophisticated, change frequently and may originate from less regulated and remote areas of the world. While we have not experienced any such system failure, theft of information, accident or security breach to date, if such an event were to occur and cause interruptions in our operations, it could result in a material disruption of our clinical development activities. For example, the loss of clinical trial data from historical or future clinical trials could result in delays in regulatory approval efforts and significantly increase costs to recover or reproduce the data. To the extent that any disruption, theft of information, or security breach were to result in a loss of or damage to data or applications, or inappropriate disclosure of confidential or proprietary information, we could incur liability and the clinical development and the future development of our product candidates could be delayed." Biorestorative Therapies, Inc. Form 10-K filed March 29, 2019 (SIC 8090—Services—Misc Health & Allied Services, Not Elsewhere Classified)

Cybersecurity Disclosures Relating to Actual or Known Breaches

- "On November 30, 2018, we announced a data security incident involving unauthorized access to the Starwood

reservations database (the 'Data Security Incident'). Working with leading security experts, we determined that there was unauthorized access to the Starwood network since 2014 and that an unauthorized party had copied information from the Starwood reservations database and taken steps towards removing it. The information copied from the Starwood reservations database over time included information about guests who made a reservation at a Starwood property, including names, mailing addresses, phone numbers, email addresses, passport numbers, payment card numbers and expiration dates, Starwood Preferred Guest account information, dates of birth, gender, arrival and departure information, reservation dates, and communication preferences. The combination of information varied by guest. Based on our analysis as of the date of this filing, we believe that the upper limit for the total number of guest records involved in this incident is approximately 383 million records. In many instances, there appear to be multiple records for the same guest, so we have concluded with a fair degree of certainty that information for fewer than 383 million unique guests was involved, although we are currently unable to quantify that lower number because of the nature of the data in the database. Based on our analysis as of the date of this filing, we believe that the information accessed by an unauthorized third party included approximately 5.25 million unencrypted passport numbers, approximately 18.5 million encrypted passport numbers and approximately 9.1 million encrypted payment card numbers (approximately 385,000 of which cards were unexpired as of September 2018). Certain data analytics work continues, including by the investigative firm engaged on behalf of the payment card networks, and based on the preliminary information we have as of the date of this filing, we believe that the information accessed by an unauthorized third party could include several thousand unencrypted payment card numbers.

Upon receiving information that an alert from an internal security tool was related to an attempt to access the Starwood reservations database, we quickly engaged leading security experts to conduct a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted, and assist with containment measures. While that forensic review of the incident is now complete, certain data analytics work continues. We reported this incident to law enforcement and continue to support their investigation. We have completed the planned phase out of the operation of the Starwood reservations database, effective as of the end of 2018.

Following the Data Security Incident, we began a guest outreach effort and offered certain services to help guests monitor and protect their information. Promptly following our announcement of the incident, we began sending emails on a rolling basis directly to various Starwood guests whose email addresses were in the Starwood reservations database, and we completed sending these emails on December 21, 2018. We also established a multi-language dedicated website and multi-language call center to answer guests' questions about the incident. The dedicated website provides guests details of the incident, the information affected, the steps being taken to investigate, FAQs and information about how guests can monitor and protect their information. We are offering free web monitoring solutions for affected guests in certain jurisdictions where the monitoring services are available.

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

We are currently unable to estimate the range of total possible financial impact to the Company from the Data Security Incident. However, we do not believe this incident will impact our long-term financial health. We maintain insurance designed to limit our exposure to losses such as those related to the Data Security Incident. We expect that the cost of such insurance will increase significantly in 2019 and 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, increased expenses and capital investments for IT and information security, incident response and customer care, and increased expenses for insurance, compliance activities, and to meet increased legal and regulatory requirements." Marriott International, Inc., Form 10-K filed March 1, 2019 (SIC 7011—Hotels & Motels)

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

- "During May 2018 and as disclosed in our Form 10-Q for the quarter ended March 31, 2018, we were the subject of a targeted email phishing campaign that led

to a business email compromise, pursuant to which an unauthorized party gained access to an external third-party system used by a subsidiary that we acquired in 2017. The incident resulted in the diversion of approximately $6.0 million, net of recovered funds, intended for disbursement to three clients. We immediately restored all funds to the client accounts. During the quarter ended June 30, 2018, we remediated the material weakness that gave rise to the incident and implemented additional preventive and detective control procedures.

We maintain insurance coverage to limit our losses related to criminal and network security events. During January 2019, we received approximately $1.0 million from our primary insurance carrier as a partial repayment toward our losses from the business email compromise. We are currently involved in discussions with our insurance carrier regarding coverage of the remaining losses, and intend to vigorously pursue repayment of these losses. Due to the ongoing discussions with our insurance carrier and the uncertainty regarding timing and full collectability of the loss, we recorded an allowance of $5.0 million for the remaining amount of the loss, which is included in the line 'General and administrative' in the accompanying Consolidated Statements of Operations. For the year ended December 31, 2018, total charges from the phishing incident included in our Consolidated Statements of Operations were $5.4 million for losses and related expenses that are not probable of recovery." RealPage, Inc., Form 10-K filed February 27, 2019 (SIC 7372—Services—Prepackaged Software)

- "[. . .] This material weakness is due to cybersecurity breaches from email spoofing. As a result, management concluded that our internal control over reporting was not effective as of December 31, 2018. Management has developed a remediation plan to address the material weaknesses related to its processes and procedures surrounding the accounting for complex financial instruments and derivatives, accounting for complex sales distribution agreements, accounting for equity component of service agreements and ensuring that generally accepted accounting principle disclosures are complete and accurate. The remediation plan consists of, among other things, engaging a third-party financial reporting consulting firm to assist the Company in its financial reporting compliance and redesigning the procedures to enhance the identification, capture, review, approval and recording of terms and components of complex financial instruments and derivatives, complex sales distribution agreements, and any equity components of service agreements as well as identify necessary disclosures. Management has engaged a third-party consultant, who is a technical accounting professional, to assist us in the interpretation and application of new and complex accounting guidance. Management will continue to review and make necessary changes to the overall design of our internal control environment. These measures are intended both to address the identified material weaknesses and to enhance our overall internal control environment.

  Management will develop a remediation plan to address the material weakness related to its information technology infrastructure. The remediation plan will include, but not be limited to cybersecurity training for all employees and redesign of procedures that cybersecurity breaches may impact." SANUWAVE Health, Inc., Form 10-K filed April 1, 2019 (SIC 3841—Surgical & Medical Instruments & Apparatus)

Disclosure regarding Ongoing Litigation Related to Cybersecurity Breaches

- "The Company treats cybersecurity risk seriously. The Company has a program to identify, mitigate and manage its cybersecurity risks. The program includes penetration testing and vulnerability assessment, technological defenses such as antivirus software, patch management, firewall management, email and web protections, an intrusion prevention system, a cybersecurity insurance policy which covers some but not all losses arising from cybersecurity breaches, as well as ongoing employee training. The costs of these measures were $224 for the twelve months ended December 31, 2018 and $153 for the twelve months ended December 31, 2017. These costs are included in various categories of noninterest expense.

  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 currently recognizes an insurance receivable in other assets of $50. The insurance carrier offered a settlement of $50 in 2018 and the Company filed suit to recover additional amounts. Litigation procedures were in process as of December 31, 2018. Costs for investigation, remediation, and legal consultation totaled $224 in 2018, $407 in 2017 and $46 in 2016. The Company's litigation against the insurance carrier was settled during the first quarter of 2019, subject to a non-disclosure agreement. As of December 31, 2018, the Company has appropriately accounted for the breaches. There has been no litigation against the Company to date associated with the breaches.

We have deployed a multifaceted 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 cyberintrusions. However, it is not possible to fully eliminate exposure. The potential for financial and reputational losses due to cybersecurity breaches is increased by the possibility of human error, unknown system susceptibilities, and the rising sophistication of cybercriminals 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 March 13, 2019 (SIC 6021—National Commercial Banks)

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

Market Outlook

Cybersecurity Breach Disclosure Enhancements

With the constant evolution of technology in the cyber world, the risks and costs associated with cybersecurity will continue to grow. Investors and regulators are demanding more robust disclosure regarding cybersecurity risks and incidents. Here is some practical advice on preparing the required disclosures regarding cybersecurity risks and incidents in SEC-filed documents:

- **Develop a tailored approach to determine the materiality of cybersecurity risks or incidents.** A public company should consider carefully the factors that are particular to the company or its industry and develop a tailored framework in evaluating the materiality of cybersecurity risks or incidents. While a public company may consider the approaches taken by other public companies, it cannot simply rely on approaches taken by other companies in determining whether cybersecurity risk poses a material risk. For example, public companies that have a strong e-commerce presence, that outsource business functions, that handle personal data, that handle financial transactions, that handle health related records, that has public safety concerns due to the nature of the industry it is in, or that have insurance covering cybersecurity events should make additional disclosure to that effect. In addition, companies should resist the temptation of adding boilerplate cybersecurity disclosure that is not meaningful to investors.
- **Disclose the costs associated with cybersecurity efforts.** Companies should consider disclosing the costs of ongoing cybersecurity efforts and the costs and consequences of cybersecurity incidents. These include but are not limited to costs of preventative measures; costs associated with investigations, regulatory proceedings, and litigation; loss of intellectual property; and costs of remediation efforts. Companies also should take into account such information in preparing MD&A disclosure and financial statements (e.g., identifying contingencies).
- **Balance the desire for particularity and the need for protection of 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 may give a potential hacker a road map for cyberattack. Public companies are not required to make detailed disclosures that could compromise their cybersecurity efforts.

- **Make timely and ongoing disclosure if a cyber incident occurs.** After a material cyber incident, a company should provide notice to investors (e.g., a current report on Form 8-K or 6-K) in an appropriate time frame. The notice should provide accurate and sufficient disclosures of material information without harming the company competitively. The fact that there is an ongoing internal or external investigation should not by itself form the basis for delaying otherwise required disclosure regarding the occurrence of a material event. For further information on timely disclosure, see Duties to Disclose and Update Disclosure.
- **Reassess internal control to account for cybersecurity related threats over assets of public companies.** While the challenges brought by cybersecurity risks may be new, the SEC expects public companies to maintain effective internal control over financial reporting and monitor those controls updated as cybersecurity risks evolve. When devising and maintaining a system of internal accounting controls, public companies should evaluate whether their internal accounting control systems are sufficient to provide reasonable assurance in safeguarding their assets from cybersecurity related risks. For example, transactions should be executed in accordance with management's general or specific authorization. Responsible personnel should be trained to understand and follow the company's procedures to avoid cybersecurity fraud.

Mingli Wu, Staff Attorney, Mayer Brown LLP

Mingli Wu is a Corporate & Securities staff attorney in Mayer Brown's New York office. He focuses on structured products linked to equities, currencies, and interest rates; debt security offerings and asset backed securities.

Prior to joining Mayer Brown, Mingli served as a law clerk to Presiding Judge Scott Myren, Judge Jon Flemmer, Judge Tony Portra and Judge Richard Sommers in the Fifth Judicial Circuit of South Dakota (2016-2017), and was an anti-money laundering compliance attorney for a global casino and resort company based in Las Vegas, Nevada. In China, he worked as in-house counsel and corporate secretary to a state-owned enterprise in Zhejiang Province, advising organization members on corporate governance, contract and operation management. He was also a legal consultant on foreign direct investment for a consulting firm in Beijing.

Mingli has Legal Profession Qualification Certificate issued by Ministry of Justice of China. He is fluent in Mandarin Chinese.

Hanwen Zhang, Staff Attorney, Mayer Brown LLP

Hanwen Zhang is a staff attorney in Mayer Brown's New York office and a member of the Corporate & Securities practice. She focuses on debt securities offerings by financial institutions under continuous offering programs that are registered under the Securities Act or that are exempt from registration under Rule 144A and Section 3(a)(2) of the Securities Act. She advises clients on securities offerings of structured products linked to equities, commodities, interest rates, currencies and other underlying assets.