Market Trends 2017/18: Cybersecurity Related Disclosures

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


Mingli Wu


Hanwen Zhang

On February 21, 2018, nearly seven years after the original issuance of guidance relating to disclosure of cybersecurity risks and cyber incidents, the Securities and Exchange Commission (SEC) released a statement and interpretive guidance regarding disclosures on cybersecurity risks and incidents (2018 guidance). The 2018 guidance reinforces and expands the SEC's prior guidance regarding cybersecurity disclosures. It is likely that the SEC's recent guidance reflects an increased interest, both from a disclosure perspective, as well as from an enforcement perspective, on the responses of public companies to cybersecurity risks and incidents. This market trends article identifies some representative cybersecurity disclosures and concludes with recommendations for enhancing cybersecurity-related disclosures moving forward. The company name, its industry, and the type of filing accompany each sample disclosure for reference.

The 2018 guidance reminds public companies of their obligation 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 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 and incidents.

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. 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—Cybersecurity risks. Set forth below are some examples of cybersecurity disclosures in the Risk Factor section:

General Disclosure on Cybersecurity Risks

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

  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-Q filed April 26, 2018 (SIC 7389—Services—Business Services)*

- **"Risks Related to Cybersecurity.**

  Increased reliance on technology by both the Fund and its service providers have resulted in increased risks posed to their respective information systems. The Fund and its service providers are susceptible to cyber-security risks including, among other things, theft, unauthorized monitoring, release, misuse, loss, destruction or corruption of confidential and highly restricted data; denial of service attacks; unauthorized access to relevant systems; compromises to networks or devices that the Fund and its service providers use to service the Fund's operations; or operational disruption or failures in the physical infrastructure or operating systems that support the Fund and its service providers. Cyber-attacks against or security

breakdowns of the Fund or its service providers may adversely impact the Fund and its shareholders, potentially resulting in, among other things, financial losses; the inability of Fund shareholders to transact business and the Fund to process transactions; inability to calculate a Portfolio's NAV; violations of applicable privacy and other laws; regulatory fines, penalties, reputational damage, reimbursement or other compensation costs; and/or additional compliance costs. The Fund may incur additional costs for cyber security risk management and remediation purposes. In addition, cyber security risks may also impact issuers of securities in which a Portfolio invests, which may cause a Portfolio's investment in such issuers to lose value. There can be no assurance that the Fund or its service providers will not suffer losses relating to cyber-attacks or other information security breaches in the future." *Venture Lending & Leasing IX, Inc., Form 10-K filed March 16, 2018*

- **"Our business depends on the Internet, our infrastructure and transaction-processing systems.**

  We are completely dependent on our infrastructure and on the availability, reliability and security of the Internet and related systems. Substantially all of our computer and communications hardware is located at a single Overstock-owned and -operated facility . . . . Our back-up facility is not adequate to support sales at a high level. Our servers and applications are vulnerable to malware, physical or electronic break-ins and other disruptions, the occurrence of any of which could lead to interruptions, delays, loss of critical data or the inability to accept and fulfill customer orders. Any system interruption that results in the unavailability of our Website or our mobile app or reduced performance of our transaction systems could interrupt or substantially reduce our ability to conduct our business. We have experienced periodic systems interruptions due to… intentional cyber-attacks in the past, and may experience additional interruptions or failures in the future. Any failure or impairment of our infrastructure or of the availability of the Internet or related systems could have a material adverse effect on our financial results and business." *Overstock.com, Inc, Form 10-K filed March 15, 2018 (SIC 5961—Retail—Catalog & Mail-Order Houses)*

- **"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. 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 goes 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, 2018 (SIC 6282—Investment Advice)*

- **"Our operations may be adversely affected by cybersecurity risks.**

  We are subject to cybersecurity risks including unauthorized access to privileged information, technological assaults on our infrastructure aimed at stealing information, fraud or interference with regular service and interruption of our services to clients or users resulting from the exploitation of these vulnerabilities. Cyber-attacks, distributed denial of service attacks and other cybersecurity matters, if successful, could have an adverse effect on our business, financial condition or results of operations. Two of the most significant cyber-attack risks that we face are e-fraud and loss of sensitive customer data. Loss from e-fraud occurs when cyber-criminals extract funds directly from clients' or our accounts using fraudulent schemes that may include Internet-based funds transfers. Such attacks are infrequent, but could present significant reputational, legal and regulatory costs to us if successful. We also face risks related to cyber-attacks and other security breaches in connection with credit card transactions that typically involve the transmission of sensitive information regarding our clients through various third parties, including merchant acquiring banks, payment processors, payment card networks, our processors and clearing banks. Some of these parties have in the past been the target of security breaches and cyber-attacks, and because the transactions involve third parties and environments such as the point of sale that we do not control or secure, future security breaches or cyber-attacks affecting any of these third parties could impact us through no fault of our own, and in some cases we may have exposure and suffer losses for breaches or attacks relating to them. Additionally, we face the risk that a party with which we or our clients do business, such as credit rating agencies, could suffer a cyber-attack. If such a cyber-attack occurs, we could be indirectly impacted in a variety of ways, such as our clients' personal data is compromised or consumer confidence is undermined.

  We cannot assure you that we will not experience a material cyber-attack, suffer indirect consequences from a cyber-attack on a third party, or fail to anticipate, identify or offset such threats of potential cyber-attacks or breaches of our security in a timely manner. If such an event occurs, our financial condition and results of operations could be materially and adversely affected." *FirstCaribbean International Bank Ltd., Form F-1 filed March 23, 2018 (SIC 6029—Commercial Banks)*

- **"We are subject to cyber security risks and may incur increasing costs in an effort to minimize those risks.**

  […] Although we take steps to secure our management information systems, and although multiple auditors review and approve the security configurations and management processes of these systems, including our computer systems, intranet and internet sites, email and other telecommunications and data networks, the security measures we have implemented may not be effective, and our systems may be vulnerable to theft, loss, damage and interruption from a number of potential sources and events,

including unauthorized access or security breaches, natural or man-made disasters, cyberattacks, computer viruses, power loss, or other disruptive events. We may not have the resources or technical sophistication to anticipate or prevent rapidly evolving types of cyberattacks. Attacks may be targeted at us, our customers and suppliers, or others who have entrusted us with information. In addition, attacks not targeted at us, but targeted solely at suppliers, may cause disruption to our computer systems or a breach of the data that we maintain on customers, employees, suppliers and others.

Actual or anticipated attacks may cause us to incur increasing costs, including costs to deploy additional personnel and protection technologies, train employees and engage third-party experts and consultants, or costs incurred in connection with the notifications to employees, suppliers or the general public as part of our notification obligations to the various governments that govern our business. Advances in computer capabilities, new technological discoveries, or other developments may result in the breach or compromise of technology used by us to protect transaction or other data. In addition, data and security breaches can also occur as a result of non-technical issues, including breaches by us or by persons with whom we have commercial relationships that result in the unauthorized release of personal or confidential information. Our reputation, brand and financial condition could be adversely affected if, as a result of a significant cyber event or other security issues: our operations are disrupted or shut down; our confidential, proprietary information is stolen or disclosed; we incur costs or are required to pay fines in connection with stolen customer, employee or other confidential information; we must dedicate significant resources to system repairs or increase cyber security protection; or we otherwise incur significant litigation or other costs." *Spirit Airlines, Inc., Form 424B2 filed November 14, 2017 (SIC 4512—Air Transportation, Scheduled)*

Disclosures Relating to Cybersecurity Incidents

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

  In May 2014, we publicly announced that criminals were able to penetrate and steal certain data, including user names, encrypted user passwords and other non-financial user data. Upon making this announcement, we required all buyers and sellers on our platform to reset their passwords in order to log into their account. The breach and subsequent password reset have negatively impacted the business. In July 2014, a putative class action lawsuit was filed against us for alleged violations and harm resulting from the breach. The lawsuit was recently dismissed with leave to amend. In addition, we have received requests for information and are subject to investigations regarding this incident from numerous regulatory and other government agencies across the world." *eBay Inc., Form 10-Q filed April 26, 2018 (SIC 7389—Services—Business Services)*

- **"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 cyber-attacks or other information security breaches such as the one that occurred in July 2017, we have been the subject of a successful hacking and cyber-attack 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 cyber-attack 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 cyber-attack 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." *Southern National Bancorp of Virginia, Inc. 10-K (FY 2017) filed March 16, 2018 (SIC 6022—State Commercial Banks)*

- **"Any failure by us to protect student photos and 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.**

  […] Our expanded use of cloud-based services (such as AWS) could also increase the risk of security breaches as cyber-attacks on cloud environments are increasing to almost the same level as attacks on traditional information technology systems. For example, in 2014, we experienced a cyber-attack 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 is able to 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. Additionally, although we have taken remediation and precautionary measures to prevent this type of situation from occurring again, we cannot guarantee that these measures measures [sic] will be effective." *Shutterfly, Inc., Form 10-Q filed May 10, 2018 (SIC 7384—Services—Photofinishing Laboratories)*

- **"Security breaches like the cybersecurity incident announced in September 2017 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 U.S., Canadian and U.K. consumers… Following the cybersecurity incident, we began undertaking significant remediation efforts and other steps to enhance our data security infrastructure. In connection with these efforts, we have incurred significant costs and expect to incur additional significant costs as we take further steps to prevent unauthorized access to our systems and the data we maintain. The actions we have taken are based on our investigation of the causes of the cybersecurity incident, but there will be additional changes needed to prevent a similar incident. We cannot assure that all potential causes of the incident have been identified and remediated and will not occur again." *Equifax Inc., Form 10-K filed March 1, 2018 (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.**

  Until the data breach we experienced in the fourth quarter of 2013, all incidents we encountered were insignificant. The data breach we experienced in 2013 was significant and went undetected for several weeks. Both we and our vendors had data security incidents subsequent to the 2013 data breach; however, to date these other incidents have not been material to our consolidated financial statements. 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 breaches or fail to detect and appropriately respond to significant data security breaches, 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, which could cause them to discontinue using our REDcards or loyalty programs, or stop shopping with us altogether." *Target Corp., Form 10-K filed March 14, 2018 (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 during 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—Item 1. Description of Business. 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:

- "Most states have also adopted data security breach laws that require notice to affected consumers of any security breach as to their personal information. In the event of a security breach, our compliance with these laws may subject us, depending on the personal information in question, to costs associated with notice and remediation, as well as potential investigations from federal regulatory agencies and state attorneys general. Failures to safeguard data adequately or to destroy data securely could subject us to regulatory investigations or enforcement actions under federal or state data security, unfair practices, or consumer protection laws. The scope and interpretation of these laws, and the burdens and costs of complying with them, could increase in the future." *Avalara, Inc., Form S-1/A filed June 13, 2018 (SIC—7372—Services - Prepackaged Software)*

- "While 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 be independently discovered by competitors. To the extent that our consultants, contractors or collaborators 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." *Autolus Therapeutics Limited, Form F-1/A filed June 8, 2018 (SIC—2836—Biological Products, (Except Diagnostic Substances))*
- "The Corporation is under continuous threat of cyber-attacks especially as we continue to expand customer services via the internet and other remote service channels. Three of the most significant cyber-attack risks that we face are e-fraud, denial-of-service and computer intrusion that might result in loss of sensitive customer data. Loss from e-fraud occurs when cybercriminals breach and extract funds from customer bank accounts. Denial-of-service disrupts services available to our customers through our on-line banking system. Computer intrusion attempts might result in the breach of sensitive customer data, such as account numbers and social security numbers, and any cyber-attacks could present significant reputational, legal and/or regulatory costs to the Corporation if successful. Our risk and exposure to these matters remains heightened because of the evolving nature and complexity of the threats from organized cybercriminals and hackers, and our plans to continue to provide electronic banking services to our customers.

  If personal, non-public, confidential or proprietary information of our customers in our possession were to be mishandled or misused, we could suffer significant regulatory consequences, reputational damage and financial loss. Such mishandling or misuse could include, for example, the erroneous provision of information to parties who are not permitted to have the information, either by fault of our systems, employees, or counterparties, or the interception or other inappropriate use of such information by third parties." *First BanCorp (Puerto Rico), Form 10-K filed March 16, 2018 (SIC—Industry: 6022 State Commercial Banks)*
- "We maintain certain computer networks, computer systems and databases in connection with our business operations and services. We use readily available third party security programs to protect these systems and databases and we periodically review security measures. Any security system or program may be vulnerable to hacking or security breaches, especially since hacking and malicious programs are constantly evolving to overcome new security measures. Like any company's computer and network systems and databases, our systems and databases could be vulnerable to security hacking or malicious programs. We may also be vulnerable to security leaks and violations by employees and contractors, which is a threat faced by all IT Business companies. We have not experienced any significant security breaches or problems as of the date of filing of this Annual Report on Form 10-K. VEII technical staff typically evaluates cybersecurity and security measures from time to time as new threats become known to us." *Value Exchange International, Inc., Form 10-K filed April 16, 2018 (SIC 7380—Services—Miscellaneous Business Services)*

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

- "As with any business, many aspects of our operations are subject to influences outside our control. These factors include, without limitation, national, regional and local economic conditions affecting consumer spending, … potential judgments, fines, legal fees and other costs, breach of information systems or theft of employee or customer data, ongoing and potential future legal or regulatory proceedings, management of our information systems, failure to develop and implement new technologies, the failure of customer-facing technology systems, business disruption including from the implementation of supply chain technologies..." *Tractor Supply Company Form 10-Q filed May 11, 2018 (SIC 5200—Retail—Building Materials, Hardware, Garden Supply)*

Cybersecurity Risk Management Disclosures

- "Despite the implementation of security measures, those technology systems and solutions could become vulnerable to damage, disability or failures due to theft, fire, power loss, telecommunications failure or other catastrophic events. Our increasing reliance on third party systems also present the risks faced by the third party's business, including the operational, security and credit risks of those parties. If those systems were to fail or otherwise be unavailable, and we were unable to recover in a timely way, we could experience an interruption in our operations.

  Furthermore, security breaches have from time to time occurred and may in the future occur involving our systems, the systems of the parties we communicate or collaborate with (including franchisees), or those of third party providers. These may include such things as unauthorized access, denial of service, computer viruses, introduction of malware or ransomware and other disruptive problems caused by hackers. Our information technology systems contain personal, financial and other information that is entrusted to us by our customers, our employees and other third parties, as well as financial, proprietary and other confidential information related to our business. An actual or alleged security breach could result in disruptions, shutdowns, theft or unauthorized disclosure of personal, financial, proprietary or other confidential information. The occurrence of any of these incidents could result in reputational damage, adverse publicity, loss of consumer confidence, reduced sales and profits, complications in executing our growth initiatives and criminal penalties or civil liabilities." *McDonald's Corporation Form 10-Q filed May 8, 2018 (SIC 5812—Retail—Eating Places)*
- "Our operations rely on the secure receipt, processing, storage and transmission of confidential and other information in our computer systems and networks and with our business partners, including proprietary, confidential or personal information that is subject to privacy laws, regulations or contractual obligations. Information security risks for large institutions like us have significantly increased in recent years and from time to time we have been, and likely will continue to be, the target of attempted cyberattacks and other information security threats. These risks are an unavoidable result of being in business, and managing these risks is part of our business activities.

  We have developed and continue to enhance our cybersecurity risk management program to protect the security of our computer systems, software, networks and other technology assets against unauthorized attempts to access confidential information or to disrupt or degrade business operations. Our cybersecurity risk management program aligns to the COSO Enterprise Risk Management framework, the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity, and has evolved based on the changing needs of our business, the evolving threat environment and FHFA regulatory guidance. Our cybersecurity risk management program extends to oversight of third parties that could be a source of cybersecurity risk, including customers that use our systems and third-party service providers. We examine the effectiveness and maturity of our cyber defenses through various means, including internal audits, targeted testing, incident response exercises, maturity assessments and industry benchmarking. We inform our Board of Directors on a regular

basis of our cybersecurity posture, policies and practices, as well as our prioritization of cybersecurity investments. We continue to strengthen our partnerships with the appropriate government and law enforcement agencies and with other businesses and cybersecurity services in order to understand the full spectrum of cybersecurity risks in the environment, enhance our defenses and improve our resiliency against cybersecurity threats. We also have obtained insurance coverage relating to cybersecurity risks. To date, we have not experienced any material losses relating to cyberattacks.

Despite our efforts to ensure the integrity of our software, computers, systems and information, we may not be able to anticipate, detect or recognize threats to our systems and assets, or to implement effective preventive measures against all cyber threats, especially because the techniques used are increasingly sophisticated, change frequently, are complex, and are often not recognized until launched. See 'Risk Factors' for additional discussion of cybersecurity risks to our business." *Federal National Mortgage Association Form 10-K filed February 14, 2018 (SIC 6111—Federal & Federally—Sponsored Credit Agencies)*

Cybersecurity Disclosures Relating to Actual or Known 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, and firewall management, as well as ongoing employee training. In 2017, the Company also implemented additional email and web protections, an intrusion prevention system and an additional targeted cybersecurity insurance policy. The costs of these measures were $134 for the twelve months ended December 31, 2017, and $66 for the twelve months ended December 31, 2016. 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 firms provided the Company with recommendations concerning its systems and procedures. The Company adopted and implemented all of the recommendations resulting from the investigation of the May 2016 intrusion and has implemented most of the recommendations from the investigation of the January 2017 intrusion, with targeted completion for all such recommendations in 2018.

  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 within other operating expenses, and currently recognizes an insurance receivable in other assets of $2,061. The Company filed an insurance claim in 2017 for both of the breaches and is awaiting a response from the insurance company. The Company has had no adverse communication from the insurance company. Costs for investigation, remediation, and legal consultation totaled $407 in 2017 and $46 in 2016. As of December 31, 2017, the Company has appropriately accounted for the breaches. There has been no litigation 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 has adopted new protections and invested additional resources to increase its security." *National Bankshares, Inc., Form 10-K (FY 2017) filed March 14, 2018 (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 online presence, outsource business functions, handle personal data, handle financial transactions, handle health related records, or 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.

Mingli Wu
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
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.