Ballard Spahr LLP

Cybersecurity Disclosure in Municipal Offerings

The Municipal Securities Disclosure Series, Part II

William C. Rhodes
Partner, Public Finance
Municipal Securities Regulation and Enforcement
215.864.8534 | rhodes@ballardspahr.com

Kimberly D. Magrini,
Associate, Public Finance
Municipal Securities Regulation and Enforcement
215.864.8365 | magrinik@ballardspahr.com

Cybersecurity Disclosure in Municipal Offerings

October 2019
By William C. Rhodes and Kimberly D. Magrini

Background. Cybersecurity is one of the leading discussion topics in municipal securities disclosure. Recently, regulators in the Office of Municipal Securities of the Securities and Exchange Commission (SEC) have repeatedly and publicly expressed concerns about the adequacy of municipal offering disclosures relating to data protection given the increasing frequency and sophistication of cybersecurity and data breaches and the requirements for corporate registrants to include line-item disclosures on this topic in their SEC filings. Additionally, the results of cybersecurity attacks are negatively affecting municipal issuer credit ratings—S&P lowered the outlook on Princeton Community Hospital (BBB+) in West Virginia to "Negative" in April 2019 because of a ransomware attack that cost $10.8 million, per management's estimates. Cybersecurity concerns have also been raised at the federal government level; the State and Local Government Cyber-security Act, currently proposed in the Senate, is expected to be considered by lawmakers in the current federal legislative session and seeks to create a grant program housed in the Department of Homeland Security for state and local governments.

Adequacy of disclosure is assessed based upon a standard of materiality. Courts have found that information is material to investors if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision. In assessing whether *omitted* information (more relevant to this topic) would have been material, courts consider whether there is a substantial likelihood that the disclosure of the omitted information would have been viewed by a reasonable investor as having significantly altered the total mix of information available. The "total mix of information" includes information known or reasonably available to investors, including information reported in the press, published reports by private experts or public officials, or information otherwise available in the public domain. Materiality may depend on the range of damage or harm that could result from the risks, including increased operating costs associated with mitigation strategies (operational changes, additional personnel, training, third-party consultants, etc.), repairs to damaged facilities, legal risks and litigation expenses, lost revenue, increased insurance premiums, reputational harm, reduced competitiveness, or changes in the market value of public debt securities.

The lack of robust, consistent disclosure on cybersecurity in municipal offerings may be attributable to a number of factors, including lack of certainty of the potential impacts of cyber threats, misunderstanding of the issues by individuals preparing disclosures, perceived secrecy of cyber threat mitigation measures, and expectations of future mitigation strategies. These and other factors, whether accurate or not, have resulted in widespread inconsistency and lack of urgency in obligated parties' approaches to disclosure. Through May 2019, at least 24

municipalities had already reported ransomware attacks. Furthermore, increased use and reliance on artificial intelligence machine learning creates more vulnerabilities in computer networks, contributing to the potential for more frequent cybersecurity attacks in the future. The increasing frequency and sophistication of cybersecurity attacks, not only on corporate borrowers but also on government agencies and municipalities, underscores the need for comprehensive disclosure related to the risks, impacts, and mitigation efforts to defend against cybersecurity attacks.

Municipal issuers seem reluctant to fully disclose their cybersecurity risks and mitigation efforts in their offering documents. A typical excuse is that an issuer may not want to reveal its cyber threat mitigation strategy, leaving investors to wonder if there is any mitigation strategy at all. Issuers (and underwriters) do not need to disclose technical cyber threat countermeasures; however, disclosure of the recognized potential risks from such threats and general approaches by an obligated party to address such risks may be material to prospective investors. By way of comparison, corporate registrants have been ahead of the municipal curve in cybersecurity disclosure. Attached as Exhibit A is an example of robust cybersecurity disclosure by a corporate registrant.

Disclosures on risks usually take two complementary forms: (1) risk matters/investment considerations and (2) management discussion of mitigation strategies to reduce those risks. These are two different types of disclosures, but issuers and underwriters should consider them in tandem to convey fully to prospective investors the likelihood and potential magnitude of the risks, as well as the nature and efficacy of the responses undertaken by an issuer to address the perceived risks. Investors will want to assess both the adequacy (and reasonableness) of the disclosure for the level of risk and the nature and quality of the management capabilities and efforts of the issuer.

Below are recent examples of effective elements of cybersecurity disclosures identified from a diverse sampling of public debt offerings around the country. These examples have been selected to present different risks and specific elements of effective disclosure. Taken together, they serve to highlight various disclosures that market participants should consider in drafting their own disclosure of cybersecurity risks and mitigation strategies.

Cybersecurity Disclosure. Recent headlines have demonstrated that certain sectors within the municipal market, including health systems and governmental enterprises, have been targeted (and victimized) by hackers demanding "ransom" payments to allow the entities to regain access to and control over their electronic records. As is often the case in the municipal securities market, practitioners should consider the relevant required line-item disclosures by public corporations in their SEC filings and registration statements.

While the vast majority of municipal bond disclosures on cybersecurity fall well short of the corporate registrant disclosures set forth in Exhibit A, below is a rather comprehensive cybersecurity risk disclosure from a recent health system offering in South Carolina.

> ***Cybersecurity Risk***
>
> *In the provision of services, hospitals create, use and maintain electronic health data and financial data on equipment, networks and corporate systems and share such information with third party servicers. This subjects hospitals to potential cybersecurity risks from outside unrelated parties, within the workforce and from faulty equipment and services. Healthcare institutions have been targeted by outside third parties, including technically sophisticated and well-resourced state-sponsored actors, attempting to access*

or compromise systems and to steal patient data. This can include hacks and malware. Outside parties may attempt to fraudulently induce the hospital employees, partners, or other parties to disclose sensitive information or take other actions to gain access to data (including patients' data). This can take the form of ransomware. In addition, hospital employees, some of whom have access to protected health information and other personally identifiable information, have in the past received "phishing" emails intended to trick recipients into surrendering their user names and passwords. Phishing is a fraud method in which the perpetrator sends out legitimate-looking emails in an attempt to gather personal, business, financial or other information from recipients.

A hospital's workforce may also constitute a threat due to inadvertent, negligent or malicious disclosure of information. Such unauthorized access or conduct may continue undetected for an extended period of time.

Hardware, software, or applications that hospitals procure from third parties to enable them to process protected health information or personally identifiable information, or which are connected to systems that hold such information, may contain defects in design or manufacture or other problems that could unexpectedly compromise network and data security. Alternatively, such problems could be the result of faulty implementation due to human error or malicious acts. In addition, if third party providers who process protected health information or personally identifiable information on a hospital's behalf, including cloud service providers, fail to adopt or adhere to adequate data security practices, or otherwise incur a breach of their networks, the hospital's data or patients' data may be improperly accessed, used, or disclosed.

The Obligated Group has taken steps to prevent unauthorized data disclosure or access to their systems; however, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently or may be disguised or difficult to detect, or designed to remain dormant until a triggering event, the Obligated Group may be unable to anticipate these techniques or implement adequate preventative measures.

While the Obligated Group is not aware of any security incident implicating patient data on their systems to date, the fact that hospitals are a primary target of security breaches or other unauthorized access or actions exposes them to a risk of theft of patient data, regulatory actions, litigation, investigations, remediation costs, damage to reputation and brand, loss of patient or investor confidence in the security of systems and resulting fees, costs, and expenses, loss of revenue, and other potential liability that could have a significantly adverse effect on their business. Successful ransomware attacks which restrict access to patient files and records also carry the risk of slowing down or even temporarily stopping the Obligated Group's ability to provide patient care.

In addition to the federal regulatory requirements of HIPAA and HITECH discussed above, hospitals may also be subject to other federal, state and foreign legislation

governing privacy, data retention, data transfer and data protection issues, including laws or regulations mandating disclosure to law enforcement bodies and individuals. A cybersecurity attack or a breach of these laws and regulations can lead to regulatory enforcement as well as litigation, including class action lawsuits, which could adversely impact Obligated Group's business and reputation.

Below is a shorter form of disclosure used recently by the Mayo Clinic. The Mayo Clinic acknowledges a history of actual attempts by hackers to access its systems and, as in the example above, disclaims any assurance that its cybersecurity precautions will be effective.

Cybersecurity.

Like many other large organizations, Mayo Clinic relies on electronic systems and technologies to conduct its operations in support of its medical treatment activities, its finances and its research and educational activities.

In the past several years, a number of entities have sought to gain unauthorized access to electronic systems of large organizations for the purposes of misappropriating assets or personal, operational, financial or other sensitive information, or causing operational disruption. These attempts, which are increasing, include highly sophisticated efforts to electronically circumvent security measures as well as more traditional intelligence gathering aimed at obtaining information necessary to gain access.

Mayo Clinic maintains a security posture designed to deter "cyber attacks", has established an Office of Information Security, and is committed to deterring attacks on its electronic systems and responding to such attacks to minimize their impact on operations. However, no assurances can be given that Mayo Clinic's security measures will be able to prevent cyber attacks on its electronic systems, and no assurances can be given that any cyber attacks, if successful, will not have a material adverse effect on the operations or financial condition of Mayo Clinic and its affiliates.

The Port Authority of New York and New Jersey addresses cybersecurity disclosure from two directions—budgetary and risk mitigation—without assessing the likelihood or magnitude of the cyber threats it faces.

The [annual operating budget] provides for ongoing operation, maintenance, and security at all agency facilities. The budget also makes strong incremental investments in security at Port Authority facilities, in a variety of cyber-security measures and in security staffing levels across the board, all necessary for the work we operate in today. …

Additionally, the Port Authority has launched a comprehensive Cybersecurity program, which includes risk assessment, asset inventory, and network infrastructure monitoring efforts that will improve Cybersecurity, as well as increase education, prevention, detection, mitigation and recovery efforts related to cyber threats across the Port Authority's facilities.

Finally, the World Trade Center ("WTC") Director of Security, reporting to

the CSO, is responsible for a multi-layered security program that employs the use of sound operational strategies and security technology solutions. The program ensures that the key elements of the WTC campus security plan that were jointly developed by the Port Authority and the New York City Police Department are effectively implemented at the site.

The Metropolitan Water District of Southern California cybersecurity risk disclosure includes information on responsible officers and training and, given the geographic breadth of its water conveyance system, ground and air patrols. Like other obligated parties, the District also acknowledges that its threat mitigation efforts may not be effective in preventing impairment of the system due to cyber or terrorist attacks.

Cybersecurity

Metropolitan has adopted and maintains an active Cybersecurity Program ("CSP") that includes policies reviewed annually by its internal Information Security Team, Audit and independent third party auditors and consultants. Metropolitan has appointed an Information Security Manager who is responsible for overseeing the annual review of the CSP and its alignment with the strategic plan and direction of Metropolitan. Metropolitan's policies and procedures are consistent with public agency standards as well as staying aligned with governance, risk, and compliance. All Metropolitan users are required to participate in Metropolitan's Information Security education and awareness training. Metropolitan's Information Security Team is responsible for providing guidance and education on the implementation of new technologies based on Metropolitan's CSP as well as overseeing the monitoring of potential threats and vulnerabilities, utilizing and executing security controls to validate policy enforcement, protecting against virus and malware attacks, and investigating any potential unauthorized activity on Metropolitan's network. …

Security Measures

Metropolitan conducts ground and air patrols of the CRA and monitoring and testing at all treatment plants and along the CRA. Similarly, DWR has in place security measures reasonably designed to protect critical facilities of the State Water Project, including both ground and air patrols of the State Water Project.

Although Metropolitan has constructed redundant systems and other safeguards to ensure its ability to continually deliver water to its customers, and DWR has made similar efforts, a terrorist attack or other security breach against water facilities could materially impair Metropolitan's ability to deliver water to its customers, its operations, and revenues and its ability to pay its obligations.

The cybersecurity risk disclosure in the City of Charlotte, North Carolina's Charlotte Douglas International Airport official statement in 2019 is one of the more extensive disclosures among recent airport offering documents. The City of Charlotte not only addresses risks associated with the airport system's own data management and

security but also highlights that airlines serving the airport, over whose technology systems the City has no control, may experience cybersecurity breaches and attacks that adversely affect the airport.

> ***Cyber-Security***
>
> *The Airport, like many other large public and private entities, relies on a large and complex technology environment to conduct its operations, and faces multiple cybersecurity threats including, but not limited to, hacking, phishing, viruses, malware and other attacks on its computing and other digital networks and systems (collectively, "Systems Technology"). As a recipient and provider of personal, private, or sensitive information, the Airport may be the target of cybersecurity incidents that could result\ in adverse consequences to Airport and its Systems Technology, requiring a response action to mitigate the consequences.*
>
> *Cybersecurity incidents could result from unintentional events, or from deliberate attacks by unauthorized entities or individuals attempting to gain access to the Airport's System Technology for the purposes of misappropriating assets or information or causing operational disruption and damage. To mitigate the risk of business operations impact and/or damage from cybersecurity incidents or cyberattacks, the Airport invests in multiple forms of cybersecurity and operational safeguards.*
>
> *While the Airport's cybersecurity and operational safeguards are periodically tested, no assurances can be given by the City that such measures will ensure against other cybersecurity threats and attacks. Cybersecurity breaches could cause material disruption to Airport's finances or operations. The costs of remedying any such damage or protecting against future attacks could be substantial. Further, cybersecurity breaches could expose the Airport to material litigation and other legal risks, which could cause the Airport to incur material costs related to such legal claims or proceedings.*
>
> *The airlines serving the Airport and other Airport tenants also face cybersecurity threats that could affect their operations and finances. Computer networks and data transmission and collection are vital to the safe and efficient operation of the airlines that serve the Airport and other tenants of the Airport. Despite security measures, information technology and infrastructure of any of the airlines serving the Airport or any other tenants at the Airport may be vulnerable to attacks by outside or internal hackers, or breached by employee error, negligence or malfeasance. Any such breach or attack could compromise systems and the information stored thereon. Any such disruption or other loss of information could result in a disruption in the efficiency of the operation of the airlines serving the Airport and the services provided at the Airport, thereby adversely affecting the ability of the Airport to generate revenue.*

The Regulator's View. In 2015, the SEC's Office of Inspections and Examinations (OCIE) launched its Cybersecurity Examination Initiative, which involves examinations of certain *regulated* entities (including municipal securities dealers) and their cybersecurity preparation. OCIE focuses on written policies and procedures for

cybersecurity, including validating and testing that such policies and procedures are implemented and followed. In addition, OCIE staff members focus on the following six areas: (1) governance and risk assessment, (2) access rights and controls, (3) data loss prevention, (4) vendor management, (5) training, and (6) incidence response. This helps inform municipal securities dealers and obligated parties of the areas on which SEC staff members would likely focus in any investigation into the adequacy of disclosure on cybersecurity risk and management. On August 7, 2017, OCIE released a report titled "Observations from Cybersecurity Examinations," summarizing its findings from these examinations. A copy of OCIE's report can be found at https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf and is attached hereto as Exhibit B. This analysis provides a window into how the SEC may assess the adequacy of disclosures on a cybersecurity program.

For further comparative consideration, attached as Exhibit C is the SEC's February 26, 2018 interpretative guidance on cybersecurity disclosure by public companies, which sets forth an analysis of proper disclosures by public companies of cybersecurity risks and mitigation strategies. The interpretive guidance can also be found at https://www.sec.gov/rules/interp/2018/33-10459.pdf.

EXHIBIT A

Cybersecurity Disclosures by a Corporate Registrant

CYBERSECURITY:

Cybersecurity risks could adversely affect our business and disrupt our operations.

The threats to network and data security are increasingly diverse and sophisticated. Despite our efforts and processes to prevent breaches, our devices, as well as our servers, computer systems, and those of third parties that we use in our operations are vulnerable to cybersecurity risks, including cyber-attacks such as viruses and worms, phishing attacks, denial-of-service attacks, physical or electronic break-ins, employee theft or misuse, and similar disruptions from unauthorized tampering with our servers and computer systems or those of third parties that we use in our operations, which could lead to interruptions, delays, loss of critical data, unauthorized access to user data, and loss of consumer confidence. In addition, we may be the target of email scams that attempt to acquire personal information or company assets. Despite our efforts to create security barriers to such threats, we may not be able to entirely mitigate these risks. Any cyber-attack that attempts to obtain our or our users' data and assets, disrupt our service, or otherwise access our systems, or those of third parties we use, if successful, could adversely affect our business, operating results, and financial condition, be expensive to remedy, and damage our reputation. In addition, any such breaches may result in negative publicity, adversely affect our brand, decrease demand for our products and services, and adversely affect our operating results and financial condition.

WE ARE INCREASINGLY DEPENDENT ON INFORMATION TECHNOLOGY AND OUR SYSTEMS AND INFRASTRUCTURE FACE CERTAIN RISKS, INCLUDING CYBERSECURITY AND DATA LEAKAGE RISKS.

Significant disruptions to our information technology systems or breaches of information security could adversely affect our business. We are increasingly dependent on sophisticated information technology systems and infrastructure to operate our business. We also have outsourced significant elements of our operations to third parties, some of which are outside the U.S., including significant elements of our information technology infrastructure, and as a result we are managing many independent vendor relationships with third parties who may or could have access to our confidential information. The size and complexity of our information technology systems, and those of our third-party vendors with whom we contract, make such systems potentially vulnerable to service interruptions. In addition, we and our vendors could be susceptible to third party attacks on our information technology systems. Such attacks are increasingly sophisticated and are made by groups and individuals with a wide range of motives and expertise, including state and quasi-state actors, criminal groups, "hackers" and others. Any security breach or other disruption to our or our vendors' information technology infrastructure could also interfere with or disrupt our business operations, including our manufacturing, distribution, R&D, sales and/or marketing activities.

In the ordinary course of business, we and our vendors collect, store and transmit large amounts of confidential information (including trade secrets or other intellectual property, proprietary business information and personal information), and it is critical that we do so in a secure manner to maintain the confidentiality and integrity of such confidential information. The size and complexity of our and our vendors' systems and the large amounts of confidential information that is present on them also makes them potentially vulnerable to security breaches from

inadvertent or intentional actions by our employees, partners or vendors, or from attacks by malicious third parties. Maintaining the security, confidentiality and integrity of this confidential information (including trade secrets or other intellectual property, proprietary information, business information and personal information) is important to our competitive business position. However, such information can be difficult to protect. While we have taken steps to protect such information, and to ensure that the third-party vendors' on which we rely have taken adequate steps to protect such information, there can be no assurance that our or our vendors' efforts will prevent service interruptions or security breaches in our systems or the unauthorized or inadvertent wrongful use or disclosure of confidential information that could adversely affect our business operations or result in the loss, misappropriation, and/or unauthorized access, use or disclosure of, or the prevention of access to, confidential information. A breach of our or our vendors' security measures or the accidental loss, inadvertent disclosure, unapproved dissemination, misappropriation or misuse of trade secrets, proprietary information, or other confidential information, whether as a result of theft, hacking, fraud, trickery or other forms of deception, or for any other cause, could enable others to produce competing products, use our proprietary technology or information, and/or adversely affect our business position. Further, any such interruption, security breach, or loss, misappropriation, and/or unauthorized access, use or disclosure of confidential information, including personal information regarding our patients and employees, could result in financial, legal, business, and reputational harm to us and could have a material adverse effect on our business, financial condition, results of operations, cash flows, and/or ordinary share price.

If we sustain cyber-attacks or other privacy or data security incidents that result in security breaches, we could suffer a loss of sales and increased costs, exposure to significant liability, reputational harm and other negative consequences.

Our information technology may be subject to cyber-attacks, security breaches or computer hacking. Hackers and data thieves are increasingly sophisticated and operate large-scale and complex automated attacks. Experienced computer programmers and hackers may be able to penetrate our security controls and misappropriate or compromise sensitive personal, proprietary or confidential information, create system disruptions or cause shutdowns. They also may be able to develop and deploy malicious software programs that attack our systems or otherwise exploit any security vulnerabilities. Our systems and the data stored on those systems may also be vulnerable to security incidents or security attacks, acts of vandalism or theft, coordinated attacks by activist entities, misplaced or lost data, human errors, or other similar events that could negatively affect our systems and the data stored on those systems, and the data of our business partners. Further, third parties, such as hosted solution providers, that provide services to the Company, could also be a source of security risk in the event of a failure of their own security systems and infrastructure.

The costs to eliminate or address the foregoing security threats and vulnerabilities before or after a cyber incident could be significant. Our remediation efforts may not be successful and could result in interruptions, delays or cessation of service, and loss of existing or potential suppliers or customers. In addition, breaches of our security measures and the unauthorized dissemination of sensitive personal, proprietary or confidential information about the Company, our business partners or other third parties could expose us to significant potential liability and reputational harm. As threats related to cyber-attacks develop and grow, we may also find it necessary to make further investments to protect our data and infrastructure, which may impact the Company's results of operations. Although the Company has insurance coverage for protecting against cyber-attacks, it may not be sufficient to cover all possible claims, and the Company may suffer losses that could have a material adverse effect on its business. As a global enterprise, we could also be negatively impacted by existing and proposed laws and regulations, and

government policies and practices related to cybersecurity, data privacy, data localization and data protection. In addition, our customers may encourage, or require, compliance with certain security standards, such as the voluntary cybersecurity framework released by the National Institute of Standards and Technology (NIST), which consists of controls designed to identify and manage Cybersecurity risks, and we could be negatively impacted to the extent we are unable to comply with such standards.

Our business is subject to cybersecurity risks.

Our operations are increasingly dependent on information technologies and services. Threats to information technology systems associated with cybersecurity risks and cyber incidents or attacks continue to grow, and include, among other things, storms and natural disasters, terrorist attacks, utility outages, theft, viruses, phishing, malware, design defects, human error, or complications encountered as existing systems are maintained, repaired, replaced, or upgraded. Risks associated with these threats include, among other things:

- Theft or misappropriation of funds;
- loss, corruption, or misappropriation of intellectual property, or other proprietary or confidential information (including customer, supplier, or employee data);
- disruption or impairment of our and our customers' business operations and safety procedures;
- damage to our reputation with our customers and the market;
- exposure to litigation;
- loss or damage to our worksite data delivery systems; and
- increased costs to prevent, respond to or mitigate cybersecurity events.

Although we utilize various procedures and controls to mitigate our exposure to such risk, cybersecurity attacks and other cyber events are evolving and unpredictable. Moreover, we have no control over the information technology systems of our customers, suppliers, and others with which our systems may connect and communicate. As a result, the occurrence of a cyber incident could go unnoticed for a period of time.

We do not presently maintain insurance coverage to protect against cybersecurity risks. If we procure such coverage in the future, we cannot ensure that it will be sufficient to cover any particular losses we may experience as a result of such cyber attacks. Any cyber incident could have a material adverse effect on our business, financial condition and results of operations.

A cybersecurity incident could negatively impact our business and our relationships with customers and expose us to litigation risk.

We use computers in substantially all aspects of our business operations. We also use mobile devices, social networking and other online activities to connect with our employees and our customers. Such uses give rise to cybersecurity risks, including security breach, espionage, system disruption, theft and inadvertent release of information. Our business involves the storage and transmission of numerous classes of sensitive and/or confidential information and intellectual property, including customers' personal information, private information about employees, and financial and strategic information about the Company and its business partners. We also rely on a Payment Card Industry

compliant third party to protect our customers' credit card information. Further, as the Company pursues its strategy to grow through acquisitions and to pursue new initiatives that improve our operations and cost structure, the Company is also expanding and improving its information technologies, resulting in a larger technological presence and corresponding exposure to cybersecurity risk. If we fail to assess and identify cybersecurity risks associated with acquisitions and new initiatives, we may become increasingly vulnerable to such risks. Additionally, while we have implemented measures to prevent security breaches and cyber incidents, our preventative measures and incident response efforts may not be entirely effective. The theft, destruction, loss, misappropriation, or release of sensitive and/or confidential information or intellectual property, or interference with our information technology systems or the technology systems of third parties on which we rely, could result in business disruption, negative publicity, brand damage, violation of privacy laws, loss of customers, potential litigation and liability and competitive disadvantage.

EXHIBIT B

OCIE Report Titled "Observations from Cybersecurity Examinations"

NATIONAL EXAM PROGRAM
RISK ALERT

By the Office of Compliance Inspections and Examinations ("OCIE")[1]

Volume VI, Issue 5 **August 7, 2017**

This Risk Alert provides a summary of observations from OCIE's examinations of registered broker-dealers, investment advisers, and investment companies conducted pursuant to the Cybersecurity Examination Initiative announced on September 15, 2015.

OBSERVATIONS FROM CYBERSECURITY EXAMINATIONS

I. Introduction

In OCIE's Cybersecurity 2 Initiative, National Examination Program staff examined 75 firms, including broker-dealers, investment advisers, and investment companies ("funds") registered with the SEC to assess industry practices and legal and compliance issues associated with cybersecurity preparedness.[2] The Cybersecurity 2 Initiative built upon prior cybersecurity examinations, particularly OCIE's 2014 Cybersecurity 1 Initiative.[3] However, the Cybersecurity 2 Initiative examinations involved more validation and testing of procedures and controls surrounding cybersecurity preparedness than was previously performed.

The examinations focused on the firms' written policies and procedures regarding cybersecurity, including validating and testing that such policies and procedures were implemented and followed. In addition, the staff sought to better understand how firms managed their cybersecurity preparedness by focusing on the following areas: (1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response.

In general, the staff observed increased cybersecurity preparedness since our 2014 Cybersecurity 1 Initiative. However, the staff also observed areas where compliance and oversight could be improved. This Risk Alert provides a summary of the staff's observations from the Cybersecurity 2 Initiative

---

1 The views expressed herein are those of the staff of OCIE, in coordination with other staff of the Securities and Exchange Commission ("SEC" or "Commission"). The Commission has expressed no view on the contents of this Risk Alert. This document was prepared by the SEC staff and is not legal advice.

2 *See* OCIE, *Examination Priorities for 2015* (January 13, 2015) and *National Exam Program Risk Alert, OCIE's 2015 Cybersecurity Examination Initiative* (September 15, 2015). A few of the staff's observations discussed herein were previously discussed in a recent *National Exam Program Risk Alert, Cybersecurity: Ransomware Alert* (May 17, 2017).

3 *See* OCIE, *OCIE Cybersecurity Initiative* (April 15, 2014) and *National Exam Program Risk Alert, Cybersecurity Examination Sweep Summary* (February 3, 2015). The staff examined a different population of firms in the Cybersecurity 2 Initiative than those that were examined in the Cybersecurity 1 Initiative.

examinations and highlights certain issues observed as well as certain policies and procedures that the staff believes may be effective.[4]

II. Summary of Examination Observations

Among the 75 firms examined, the staff noted an overall improvement in firms' awareness of cyber-related risks and the implementation of certain cybersecurity practices since the Cybersecurity 1 Initiative. Most notably, all broker-dealers, all funds, and nearly all advisers examined maintained cybersecurity-related written policies and procedures addressing the protection of customer/shareholder records and information. This contrasts with the staff's observations in the Cybersecurity 1 Initiative, in which comparatively fewer broker-dealers and advisers had adopted this type of written policies and procedures.

In the examinations, the staff observed:

- Nearly all broker-dealers and the vast majority of advisers and funds conducted periodic risk assessments of critical systems to identify cybersecurity threats, vulnerabilities, and the potential business consequences of a cyber incident.

- Nearly all broker-dealers and almost half of the advisers and funds conducted penetration tests and vulnerability scans on systems that the firms considered to be critical, although a number of firms did not appear to fully remediate some of the high risk observations that they discovered from these tests and scans during the review period.

- All firms utilized some form of system, utility, or tool to prevent, detect, and monitor data loss as it relates to personally identifiable information.

- All broker-dealers and nearly all advisers and funds had a process in place for ensuring regular system maintenance, including the installation of software patches to address security vulnerabilities. However, the staff observed that a few of the firms had a significant number of system patches that, according to the firms, included critical security updates that had not yet been installed.

- Information protection programs at the firms typically included relevant cyber-related topics, such as:

    - *Policies and procedures*. Nearly all firms' policies and procedures addressed cyber-related business continuity planning and Regulation S-P.[5] In addition, nearly all broker-dealers and

---

[4] The examinations were conducted between September 2015 and June 2016 and generally covered the review period October 1, 2014 through September 30, 2015.

[5] *See* 17 C.F.R. Part 248, Subpart A—*Regulation S–P: Privacy of Consumer Financial Information and Safeguarding Personal Information*. *See also Disposal of Consumer Report Information*, Securities Exchange Act of 1934 ("Exchange Act") Release No. 50781, Investment Advisers Act of 1940 ("Advisers Act") Release No. 2332, Investment Company Act of 1940 ("Investment Company Act") Release No. 26685 (December 2, 2004), 69 Fed. Reg. 71321 (December 8, 2004) and *Privacy of Consumer Financial Information (Regulation S-P)*, Exchange Act Release No. 42974, Investment Company Act Release No. 24543, Advisers Act Release No. 1883 (June 22, 2000), 65 Fed. Reg. 40334 (June 29, 2000).

most advisers and funds had specific cybersecurity and Regulation S-ID[6] policies and procedures.

- *Response plans*. Nearly all of the firms had plans for addressing access incidents. In addition, the vast majority of firms had plans for denial of service incidents and unauthorized intrusions. However, while the vast majority of broker-dealers maintained plans for data breach incidents and most had plans for notifying customers of material events, less than two-thirds of the advisers and funds appeared to maintain such plans.

- All broker-dealers and a large majority of advisers and funds maintained cybersecurity organizational charts and/or identified and described cybersecurity roles and responsibilities for the firms' workforce.

- The vast majority of broker-dealers and nearly two-thirds of the advisers and funds had authority from customers/shareholders to transfer funds to third party accounts.

  - Some of the broker-dealers did not appear to memorialize their processes into written supervisory procedures. Rather, these broker-dealers appeared to have informal practices for verifying customers' identities in order to proceed with requests to transfer funds.

  - All of the advisers and funds maintained policies, procedures, and standards related to verifying the authenticity of a customer/shareholder who was requesting to transfer funds.

- Almost all firms either conducted vendor risk assessments or required that vendors provide the firms with risk management and performance reports (i.e., internal and/or external audit reports) and security reviews or certification reports. While vendor risk assessments are typically conducted at the outset of a relationship, over half of the firms also required updating such risk assessments on at least an annual basis.

III. Issues Observed

The staff observed one or more issues in the vast majority of the Cybersecurity 2 Initiative examinations. Highlighted below are issues the staff believes firms would benefit from considering in order to assess and improve their policies, procedures, and practices.

- While, as noted above, all broker-dealers and funds, and nearly all advisers maintained written policies and procedures addressing cyber-related protection of customer/shareholder records and information, a majority of the firms' information protection policies and procedures appeared to have issues. Examples included:

  - *Policies and procedures were not reasonably tailored* because they provided employees with only general guidance, identified limited examples of safeguards for employees to consider, were very narrowly scoped, or were vague, as they did not articulate procedures for implementing the policies.

---

[6] *See* 17 C.F.R. Part 248, Subpart C—*Regulation S–ID: Identity Theft Red Flags*. *See also* *Identity Theft Red Flags Rules*, Exchange Act Release No. 69359, Advisers Act Release No. 3582, Investment Company Act Release No. 30456 (April 10, 2013), 78 Fed. Reg. 23637 (April 19, 2013).

- *Firms did not appear to adhere to or enforce policies and procedures, or the policies and procedures did not reflect the firms' actual practices*, such as when the policies:
  - Required annual customer protection reviews; however, in practice, they were conducted less frequently.
  - Required ongoing reviews to determine whether supplemental security protocols were appropriate; however, such reviews were performed only annually, or not at all.
  - Created contradictory or confusing instructions for employees, such as policies regarding remote customer access that appeared to be inconsistent with those for investor fund transfers, making it unclear to employees whether certain activity was permissible.
  - Required all employees to complete cybersecurity awareness training; however, firms did not appear to ensure this occurred and take action concerning employees who did not complete the required training.

- The staff also observed Regulation S-P-related issues among firms that did not appear to adequately conduct system maintenance, such as the installation of software patches to address security vulnerabilities and other operational safeguards to protect customer records and information. Examples included:
  - *Stale Risk Assessments*. Using outdated operating systems that were no longer supported by security patches.
  - *Lack of Remediation Efforts*. High-risk findings from penetration tests or vulnerability scans that did not appear to be fully remediated in a timely manner.

IV. Elements of Robust Policies and Procedures[7]

During these examinations, the staff observed several elements that were included in the policies and procedures of firms that the staff believes had implemented robust controls. Firms may wish to consider the following elements as they could be useful in the implementation of cybersecurity-related policies and procedures.[8]

- *Maintenance of an inventory of data, information, and vendors*. Policies and procedures included a complete inventory of data and information, along with classifications of the risks,

---

[7] This is not intended to be a comprehensive list of the elements of robust cybersecurity policies and procedures. The adequacy of supervisory, compliance, and other risk management policies and procedures can be determined only with reference to the profile of each specific firm and other facts and circumstances.

[8] Firms may also wish to consider the guidance and information issued by the SEC's Division of Investment Management and the cybersecurity issues discussed in Commission orders in settled enforcement proceedings. *See, e.g.,* *IM Guidance Update: Cybersecurity Guidance* (April 2015), *In re Morgan Stanley Smith Barney LLC*, Exchange Act Release No. 78021, Advisers Act Release No. 4415 (June 8, 2016), *In re R.T. Jones Capital Equities Management Inc.*, Advisers Act Release No. 4204 (September 22, 2015), and *In re Craig Scott Capital LLC*, Exchange Act Release No. 77595 (April 12, 2016).

vulnerabilities, data, business consequences, and information regarding each service provider and vendor, if applicable.

- *Detailed cybersecurity-related instructions*. Examples included:
  - Penetration tests – policies and procedures included specific information to review the effectiveness of security solutions.
  - Security monitoring and system auditing – policies and procedures regarding the firm's information security framework included details related to the appropriate testing methodologies.
  - Access rights – requests for access were tracked, and policies and procedures specifically addressed modification of access rights, such as for employee on-boarding, changing positions or responsibilities, or terminating employment.
  - Reporting – policies and procedures specified actions to undertake, including who to contact, if sensitive information was lost, stolen, or unintentionally disclosed/misdirected.
- *Maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities*. Examples included:
  - Vulnerability scans of core IT infrastructure were required to aid in identifying potential weaknesses in a firm's key systems, with prioritized action items for any concerns identified.
  - Patch management policies that included, among other things, the beta testing of a patch with a small number of users and servers before deploying it across the firm, an analysis of the problem the patch was designed to fix, the potential risk in applying the patch, and the method to use in applying the patch.
- *Established and enforced controls to access data and systems*. For example, the firms:
  - Implemented detailed "acceptable use" policies that specified employees' obligations when using the firm's networks and equipment.
  - Required and enforced restrictions and controls for mobile devices that connected to the firms' systems, such as passwords and software that encrypted communications.
  - Required third-party vendors to periodically provide logs of their activity on the firms' networks.
  - Required immediate termination of access for terminated employees and very prompt (typically same day) termination of access for employees that left voluntarily.
- *Mandatory employee training.* Information security training was mandatory for all employees at on-boarding and periodically thereafter, and firms instituted policies and procedures to ensure that employees completed the mandatory training.
- *Engaged senior management*. The policies and procedures were vetted and approved by senior management.

V. Conclusion

Cybersecurity remains one of the top compliance risks for financial firms.[9] As noted in OCIE's 2017 priorities, OCIE will continue to examine for cybersecurity compliance procedures and controls, including testing the implementation of those procedures and controls at firms.[10]

This Risk Alert is intended to highlight for firms the risks and issues that the staff identified during examinations of broker-dealers, investment advisers, and investment companies regarding cybersecurity preparedness. In addition, this Risk Alert describes factors that firms may consider to (1) assess their supervisory, compliance and/or other risk management systems related to cybersecurity risks, and (2) make any changes, as may be appropriate, to address or strengthen such systems. These factors are not exhaustive, nor will they constitute a safe harbor. Factors other than those described in this Risk Alert may be appropriate to consider, and some of the factors may not be applicable to a particular firm's business. While some of the factors discussed in this Risk Alert reflect existing regulatory requirements, they are not intended to alter such requirements. Moreover, future changes in laws or regulations may supersede some of the factors or issues raised herein. The adequacy of supervisory, compliance, and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.

[9] *See*, *e.g.*, Investment Adviser Association, ACA Compliance Group, and OMAM, *2016 Investment Management Compliance Testing Survey* (June 23, 2016), which synthesizes 730 adviser compliance professionals' responses to 94 compliance-related questions. Q94: 88% of advisers view cybersecurity, privacy, and identity theft as the hottest compliance topic for 2016.

[10] OCIE, *Examination Priorities for 2017* (January 12, 2017).

EXHIBIT C

SEC Statement and Interpretative Guidance on Public Company Cybersecurity Disclosures

Conformed to Federal Register version

SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 229 and 249

[Release Nos. 33-10459; 34-82746]

Commission Statement and Guidance on Public Company Cybersecurity Disclosures

AGENCY: Securities and Exchange Commission.

ACTION: Interpretation.

SUMMARY: The Securities and Exchange Commission (the "Commission") is publishing interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.

DATES: Applicable: February 26, 2018

FOR FURTHER INFORMATION CONTACT: Questions about specific filings should be directed to staff members responsible for reviewing the documents the company files with the Commission. For general questions about this release, contact the Office of the Chief Counsel at (202) 551-3500 in the Division of Corporation Finance, U.S. Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549.

SUPPLEMENTARY INFORMATION:

I. Introduction

A. Cybersecurity

Cybersecurity risks pose grave threats to investors, our capital markets, and our country.[1] Whether it is the companies in which investors invest, their accounts with financial services firms, the markets through which they trade, or the infrastructure they count on daily, the investing public and the U.S. economy depend on the security and reliability of information and communications technology, systems, and networks. Com-

[1] The U.S. Computer Emergency Readiness Team defines cybersecurity as "[t]he activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." U.S. Computer Emergency Readiness Team website, available at https://niccs.us-cert.gov/glossary#C (Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May 2009).

panies today rely on digital technology to conduct their business operations and engage with their customers, business partners, and other constituencies. In a digitally connected world, cybersecurity presents ongoing risks and threats to our capital markets and to companies operating in all industries, including public companies regulated by the Commission.

As companies' exposure to and reliance on networked systems and the Internet have increased, the attendant risks and frequency of cybersecurity incidents also have increased.[2] Today, the importance of data management and technology to business is analogous to the importance of electricity and other forms of power in the past century. Cybersecurity incidents[3] can result from unintentional events or deliberate attacks by insiders or third parties, including cybercriminals, competitors, nation-states, and "hacktivists."[4] Companies face an evolving landscape of cybersecurity threats in which hackers use a complex array of means to perpetrate cyber-attacks, including the use of stolen access credentials, malware, ransomware, phishing, structured query language injection attacks, and distributed denial-of-service attacks, among other means. The objectives of cyber-attacks vary widely and may include the theft or destruction of financial assets, intellectual property, or other sensitive information belonging to companies, their customers, or their business partners. Cyber-attacks may also be directed at disrupting the operations of public companies or their business partners. This includes targeting companies that operate in industries responsible for critical infrastructure.

Companies that fall victim to successful cyber-attacks or experience other cybersecurity incidents may incur substantial costs[5] and suffer other negative consequences, which may include:

---

2 See World Economic Forum, Global Risks Report 2017, 12th Ed. (Jan. 2017), available at https://www.weforum.org/reports/the-global-risks-report-2017 (concluding that "greater interdependence among different infrastructure networks is increasing the scope for systemic failures – whether from cyber-attacks, software glitches, natural disasters or other causes – to cascade across networks and affect society in unanticipated ways."). See also PwC, "Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security Survey 2016" (Oct. 2015), available at https://www.pwccn.com/en/retail-and-consumer/rcs-info-security-2016.pdf (finding that in 2015 there was a reported 38% increase in detected information security incidents from 2014).

3 A "cybersecurity incident" is "[a]n occurrence that actually or potentially results in adverse consequences to ... an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences." U.S. Computer Emergency Readiness Team website, available at https://niccs.us-cert.gov/glossary#I.

4 One study using a sample of 419 companies in 13 countries and regions noted that 47 percent of data breach incidents in 2016 involved a malicious or criminal attack, 25 percent were due to negligent employees or contractors (human factor) and 28 percent involved system glitches, including both IT and business process failures. See Ponemon Institute and IBM Security, 2017 Cost of Data Breach Study: Global Overview (Jun. 2017), available at https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states.

5 The average organizational cost of a data breach in the United States in 2016 was $7.35 million based on the sample in the study. Id. However, the total costs a company may incur in connection with a particular cyber-attack or incident could be much higher.

- remediation costs, such as liability for stolen assets or information, repairs of system damage, and incentives to customers or business partners in an effort to maintain relationships after an attack;[6]
- increased cybersecurity protection costs, which may include the costs of making organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;
- lost revenues resulting from the unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- litigation and legal risks, including regulatory actions by state and federal governmental authorities and non-U.S. authorities;7
- increased insurance premiums;
- reputational damage that adversely affects customer or investor confidence; and
- damage to the company's competitiveness, stock price, and long-term shareholder value.

Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack. Crucial to a public company's ability to make any required disclosure of cybersecurity risks and incidents in the appropriate timeframe are disclosure controls and procedures that provide an appropriate method of discerning the impact that such matters may have on the company and its business, financial condition, and results of operations, as well as a protocol to determine the potential materiality of such risks and incidents.[8] In addition, the Commission believes that the development of effective disclosure controls and procedures is best achieved when a company's directors, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about the cybersecurity risks and incidents that the company has faced or is likely to face.

---

6 A company's costs may also include payments to perpetrators of ransomware attacks in order to attempt to restore operations or protect customer data or other proprietary information. But see Federal Bureau of Investigation, "How To Protect your Network from Ransomware," Ransomware Prevention and Response for CISOs, available at https://www.justice.gov/criminal-ccips/file/872771/download.

7 See, e.g., New York State Department of Financial Services, 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies; European Union General Data Protection Regulation, Council Regulation 2016/679, 2016 O.J. (L 119) 1.

8 See Section II.B.1 below for further discussion of disclosure controls and procedures.

Additionally, directors, officers, and other corporate insiders must not trade a public company's securities while in possession of material nonpublic information, which may include knowledge regarding a significant cybersecurity incident experienced by the company. Public companies should have policies and procedures in place to (1) guard against directors, officers, and other corporate insiders taking advantage of the period between the company's discovery of a cybersecurity incident and public disclosure of the incident to trade on material nonpublic information about the incident, and (2) help ensure that the company makes timely disclosure of any related material nonpublic information.[9] In addition, we believe that companies are well served by considering the ramifications of directors, officers, and other corporate insiders trading in advance of disclosures regarding cyber incidents that prove to be material. We recognize that many companies have adopted preventative measures to address the appearance of improper trading and we encourage companies to consider such preventative measures in the context of a cyber event.

B. CF Disclosure Guidance: Topic No. 2

In October 2011, the Division of Corporation Finance (the "Division") issued guidance that provided the Division's views regarding disclosure obligations relating to cybersecurity risks and incidents.[10] The guidance explains that, although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, companies nonetheless may be obligated to disclose such risks and incidents.[11] After the issuance of the guidance, many companies included additional cybersecurity disclosure, typically in the form of risk factors.[12]

C. Purpose of Release

In light of the increasing significance of cybersecurity incidents, the Commission believes it is necessary to provide further Commission guidance. This interpretive release outlines the Commission's views with respect to cybersecurity disclosure requirements under the federal securities laws as they apply to public

---

9 See Section II.B.2 below for further discussion of insider trading.

10 See CF Disclosure Guidance: Topic No. 2 – Cybersecurity (Oct. 13, 2011), available at https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

11 Id.

12 For example, Willis North America released a 2013 report that found that approximately 88% of the public Fortune 500 companies and about 78% of the Fortune 501-1000 companies included risk factor disclosure regarding cybersecurity in their annual reports filed in 2012. See Willis Fortune 1000 Cyber Disclosure Report (Aug. 2013), available at http://blog.willis.com/wp-content/uploads/2013/08/Willis-Fortune-1000-Cyber-Report_09-13.pdf. In 2015, over 88% of Russell 3000 companies disclosed cybersecurity as a risk. See Audit Analytics, "Cybersecurity Disclosure in Risk Factors," (Jan. 14, 2016), available at http://www.auditanalytics.com/blog/cybersecurity-disclosures-in-risk-factors/.

operating companies.[13] While the Commission continues to consider other means of promoting appropriate disclosure of cyber incidents, we are reinforcing and expanding upon the staff's 2011 guidance. In addition, we address two topics not developed in the staff's 2011 guidance, namely the importance of cybersecurity policies and procedures and the application of insider trading prohibitions in the cybersecurity context.

First, this release stresses the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents. Companies are required to establish and maintain appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity. Such robust disclosure controls and procedures assist companies in satisfying their disclosure obligations under the federal securities laws.

Second, we also remind companies and their directors, officers, and other corporate insiders of the applicable insider trading prohibitions under the general antifraud provisions of the federal securities laws and also of their obligation to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents.[14]

The Commission, and the staff through its filing review process, continues to monitor cybersecurity disclosures carefully.

II. Commission Guidance

A. Overview of Rules Requiring Disclosure of Cybersecurity Issues

1. Disclosure Obligations Generally; Materiality

Companies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure that is required in registration statements under the Securities Act of 1933 ("Securities Act") and the

---

[13] This release does not address the specific implications of cybersecurity to other regulated entities under the federal securities laws, such as registered investment companies, investment advisers, brokers, dealers, exchanges, and self-regulatory organizations. For example, in 2014 the Commission adopted Regulation Systems Compliance and Integrity, applicable to certain self-regulatory organizations, to strengthen the technology infrastructure of the U.S. securities markets. Final Rule: Regulation Systems Compliance and Integrity, Release No. 34-73639 (Nov. 19, 2014) [79 FR. 72252 (Dec. 5, 2014)], available at https://www.sec.gov/rules/final/2014/34-73639.pdf. For additional cybersecurity regulations and resources, see the Commission's website page devoted to cybersecurity issues, available at https://www.sec.gov/spotlight/cybersecurity; see also Cybersecurity Guidance; IM Guidance Update (April 2015), available at https://www.sec.gov/investment/im-guidance-2015-02.pdf (staff guidance on cybersecurity measures for registered investment companies and investment advisers).

[14] See Final Rule: Selective Disclosure and Insider Trading, Release No. 33-7881 (Aug. 15, 2000) [65 FR 51715 (Aug. 24, 2000)], available at https://www.sec.gov/rules/final/33-7881.htm.

Securities Exchange Act of 1934 ("Exchange Act"), and periodic and current reports under the Exchange Act.[15] When a company is required to file a disclosure document with the Commission, the requisite form generally refers to the disclosure requirements of Regulation S-K[16] and Regulation S-X.[17] Although these disclosure requirements do not specifically refer to cybersecurity risks and incidents, a number of the requirements impose an obligation to disclose such risks and incidents depending on a company's particular circumstances. For example:

- Periodic Reports: Companies are required to file periodic reports[18] to disclose specified information on a regular and ongoing basis.[19] These periodic reports include annual reports on Form 10-K,[20] which require companies to make disclosure regarding their business and operations, risk factors, legal proceedings, management's discussion and analysis of financial condition and results of operations ("MD&A"), financial statements, disclosure controls and procedures, and corporate governance.[21] Periodic reports also include quarterly reports on Form 10-Q,[22] which require companies to make disclosure regarding their financial statements, MD&A, and updated risk factors.[23] Likewise, foreign private issuers are required to make many of these

---

15 Listed companies also should consider any obligations that may be imposed by exchange listing requirements. For example, the NYSE requires listed companies to "release quickly to the public any news or information which might reasonably be expected to materially affect the market for its securities." See NYSE Listed Company Manual Rule 202.05 – Timely Disclosure of Material News Developments. In addition, in 2015, the NYSE, in partnership with Palo Alto Networks, published a summary of information about legal and regulatory aspects of cybersecurity governance for directors and officers of public companies. See Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers. Chicago: Caxton Business & Legal, Inc., 2015, available at https://www.securityroundtable.org/wp-content/uploads/2015/09/Cybersecurity-9780996498203-no_marks.pdf. Similarly, Nasdaq requires listed companies to "make prompt disclosure to the public of any material information that would reasonably be expected to affect the value of its securities or influence investors' decisions." See Nasdaq Listing Rule 5250(b)(1).

16 17 CFR part 229.

17 17 CFR part 210.

18 An issuer with a class of securities registered under Section 12 or subject to Section 15(d) of the Exchange Act is subject to the periodic and current reporting requirements of Section 13 and 15(d), respectively, of the Exchange Act.

19 "Congress recognized that the ongoing dissemination of accurate information by companies about themselves and their securities is essential to effective operation of the trading markets. The Exchange Act rules require public companies to make periodic disclosures at annual and quarterly intervals, with other important information reported on a more current basis. The Exchange Act specifically provides for current disclosure to maintain the currency and adequacy of information disclosed by companies." Proposed Rule: Additional Form 8-K Disclosure Requirements and Acceleration of Filing Date, Release No. 33-8106, 3-4 (Jun. 17, 2002) [67 FR 42914 (Jun. 25, 2002)].

20 17 CFR 249.310.

21 See Part I, Items 1, 1A and 3 of Form 10-K; Part II, Items 7, 8 and 9A of Form 10-K; and Part III, Item 10 of Form 10-K [17 CFR 249.310].

22 17 CFR 249.308a.

23 See Part I, Items 1 and 2 of Form 10-Q; Part II, Item 1A of Form 10-Q [17 CFR 249.308a].

same disclosures in their periodic reports on Form 20-F.[24] Companies must provide timely and ongoing information in these periodic reports regarding material cybersecurity risks and incidents that trigger disclosure obligations.

- Securities Act and Exchange Act Obligations: Securities Act and Exchange Act registration statements must disclose all material facts required to be stated therein or necessary to make the statements therein not misleading. Companies should consider the adequacy of their cybersecurity-related disclosure, among other things, in the context of Sections 11, 12, and 17 of the Securities Act, as well as Section 10(b) and Rule 10b-5 of the Exchange Act.[25]
- Current Reports: In order to maintain the accuracy and completeness of effective shelf registration statements with respect to the costs and other consequences of material cybersecurity incidents,[26] companies can provide current reports on Form 8-K[27] or Form 6-K.[28] Companies also frequently provide current reports on Form 8-K or Form 6-K to report the occurrence and consequences of cybersecurity incidents.[29] The Commission encourages companies to continue to use Form 8-K or Form 6-K to disclose material information promptly, including disclosure pertaining to cybersecurity matters. This practice reduces the risk of selective disclosure, as well as the risk that trading in their securities on the basis of material non-public information may occur.[30]

In addition to the information expressly required by Commission regulation, a company is required to disclose "such further material information, if any, as may be necessary to make the required statements, in light of the circumstances under which they are made, not misleading."[31] The Commission considers omitted information to be material if there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision or that disclosure of the omitted information would have

---

24 See Part I, Items 3.D, 4, 5 and 8 of Form 20-F; Part II, Items 15 and 16G of Form 20-F; Part III, Items 17 and 18 of Form 20-F [17 CFR 249.220f].

25 15 U.S.C. 77k; 15 U.S.C. 77l; 15 U.S.C. 77q; 15 U.S.C. 78j(b); 17 CFR 240.10b-5.

26 See Item 11(a) of Form S-3 [17 CFR 239.13] and Item 5(a) of Form F-3 [17 CFR 239.33].

27 17 CFR 249.308.

28 17 CFR 249.306.

29 "The registrant may, at its option, disclose under this Item 8.01 [of Form 8-K] any events, with respect to which information is not otherwise called for by this form, that the registrant deems of importance to security holders." 17 CFR 308.

30 See Sections II.B.2 and II.B.3 below for further discussion of insider trading and Regulation FD.

31 Rule 408 of the Securities Act [17 CFR 230.408]; Rule 12b-20 of the Exchange Act [17 CFR 240.12b-20]; and Rule 14a-9 of the Exchange Act [17 CFR 240.14a-9].

been viewed by the reasonable investor as having significantly altered the total mix of information available.[32]

In determining their disclosure obligations regarding cybersecurity risks and incidents, companies generally weigh, among other things, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of the incident on the company's operations. The materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations.[33] The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause.[34] This includes harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities.

This guidance is not intended to suggest that a company should make detailed disclosures that could compromise its cybersecurity efforts – for example, by providing a "roadmap" for those who seek to penetrate a company's security protections. We do not expect companies to publicly disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident. Nevertheless, we expect companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences. Where a company has become aware of a cybersecurity incident or risk that would be material to its investors, we would expect it to make appropriate disclosure timely and sufficiently prior to the offer and sale of securities and to take steps to prevent directors and officers (and other corporate insiders who were aware of these matters) from trading its securities until investors have been appropriately informed about the incident or risk.[35]

---

32 This approach is consistent with the standard of materiality articulated by the U.S. Supreme Court in TSC Industries v. Northway, 426 U.S. 438, 449 (1976) (a fact is material "if there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision or if it "would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available" to the shareholder).

33 For example, the compromised information might include personally identifiable information, trade secrets or other confidential business information, the materiality of which may depend on the nature of the company's business, as well as the scope of the compromised information.

34 As part of a materiality analysis, a company should consider the indicated probability that an event will occur and the anticipated magnitude of the event in light of the totality of company activity. Basic v. Levinson, 485 U.S. 224, 238 (1988) (citing SEC v. Texas Gulf Sulphur Co., 401 F. 2d 833, 849 (2d Cir. 1968)). Moreover, no "single fact or occurrence" is determinative as to materiality, which requires an inherently fact-specific inquiry. Basic, 485 U.S. at 236.

35 See Sections 7 and 10 of the Securities Act; Sections 10(b), 13(a) and 15(d) of the Exchange Act; and Rule 10b-5 under the Exchange Act [15 U.S.C 78j(b); 15 U.S.C. 78m(a); 15. U.S.C. 78o(d); 17 CFR 240.10b-5].

Understanding that some material facts may be not available at the time of the initial disclosure, we recognize that a company may require time to discern the implications of a cybersecurity incident. We also recognize that it may be necessary to cooperate with law enforcement and that ongoing investigation of a cybersecurity incident may affect the scope of disclosure regarding the incident. However, an ongoing internal or external investigation – which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident.

We remind companies that they may have a duty to correct prior disclosure that the company determines was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made[36] (for example, if the company subsequently discovers contradictory information that existed at the time of the initial disclosure), or a duty to update disclosure that becomes materially inaccurate after it is made[37] (for example, when the original statement is still being relied on by reasonable investors). Companies should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident.

We expect companies to provide disclosure that is tailored to their particular cybersecurity risks and incidents. As the Commission has previously stated, we "emphasize a company-by-company approach [to disclosure] that allows relevant and material information to be disseminated to investors without boiler-plate language or static requirements while preserving completeness and comparability of information across companies."[38] Companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors.

---

36 See Backman v. Polaroid Corp., 910 F.2d 10, 16-17 (1st Cir. 1990) (en banc) (finding that the duty to correct applies "if a disclosure is in fact misleading when made, and the speaker thereafter learns of this.").

37 See id. at 17 (describing the duty to update as potentially applying "if a prior disclosure 'becomes materially misleading in light of subsequent events'" (quoting Greenfield v. Heublein, Inc., 742 F.2d 751, 758 (3d Cir. 1984))). But see Higginbotham v. Baxter Intern., Inc., 495 F.3d 753, 760 (7th Cir. 2007) (rejecting duty to update before next quarterly report); Gallagher v. Abbott Laboratories, 269 F.3d 806, 808-11 (7th Cir. 2001) (explaining that securities laws do not require continuous disclosure).

38 See Business and Financial Disclosure Required by Regulation S-K, Release No. 33-10064 (Apr. 13, 2016) [81 FR 23915 (Apr. 22, 2016)]. See also Plain English Disclosure, Release No. 33-7497 (Jan. 28, 1998) [63 FR 6370 (Feb. 6, 1998)]; and Updated Staff Legal Bulletin No. 7: Plain English Disclosure (Jun. 7, 1999) available at https://www.sec.gov/interps/legal/cfslb7a.htm.

2. Risk Factors

Item 503(c) of Regulation S-K and Item 3.D of Form 20-F require companies to disclose the most significant factors that make investments in the company's securities speculative or risky.[39] Companies should disclose the risks associated with cybersecurity and cybersecurity incidents if these risks are among such factors, including risks that arise in connection with acquisitions.[40]

It would be helpful for companies to consider the following issues, among others, in evaluating cybersecurity risk factor disclosure:

- the occurrence of prior cybersecurity incidents, including their severity and frequency;
- the probability of the occurrence and potential magnitude of cybersecurity incidents;
- the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company's ability to prevent or mitigate certain cybersecurity risks;
- the aspects of the company's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third party supplier and service provider risks;
- the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers;
- the potential for reputational harm;
- existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies; and
- litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.

In meeting their disclosure obligations, companies may need to disclose previous or ongoing cybersecurity incidents or other past events in order to place discussions of these risks in the appropriate context. For example, if a company previously experienced a material cybersecurity incident involving denial-of-service, it likely would not be sufficient for the company to disclose that there is a risk that a denial-of-service incident may occur. Instead, the company may need to discuss the occurrence of that cybersecurity incident

---

39 17 CFR 229.503(c); 17 CFR 249.220f.

40 See Final Rule: Business Combination Transactions, Release No. 33-6578 (Apr. 23, 1985) [50 FR 18990 (May 6, 1985)].

and its consequences as part of a broader discussion of the types of potential cybersecurity incidents that pose particular risks to the company's business and operations. Past incidents involving suppliers, customers, competitors, and others may be relevant when crafting risk factor disclosure. In certain circumstances, this type of contextual disclosure may be necessary to effectively communicate cybersecurity risks to investors.

3. MD&A of Financial Condition and Results of Operations

Item 303 of Regulation S-K and Item 5 of Form 20-F require a company to discuss its financial condition, changes in financial condition, and results of operations. These items require a discussion of events, trends, or uncertainties that are reasonably likely to have a material effect on its results of operations, liquidity, or financial condition, or that would cause reported financial information not to be necessarily indicative of future operating results or financial condition and such other information that the company believes to be necessary to an understanding of its financial condition, changes in financial condition, and results of operations.[41] In this context, the cost of ongoing cybersecurity efforts (including enhancements to existing efforts), the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents, among other matters, could inform a company's analysis. In addition, companies may consider the array of costs associated with cybersecurity issues, including, but not limited to, loss of intellectual property, the immediate costs of the incident, as well as the costs associated with implementing preventative measures, maintaining insurance, responding to litigation and regulatory investigations, preparing for and complying with proposed or current legislation, engaging in remediation efforts, addressing harm to reputation, and the loss of competitive advantage that may result.[42] Finally, the Commission expects companies to consider the impact of such incidents on each of their reportable segments.[43]

4. Description of Business

Item 101 of Regulation S-K and Item 4.B of Form 20-F require companies to discuss their products, services, relationships with customers and suppliers, and competitive conditions.[44] If cybersecurity in-

---

41 17 CFR 229.303; 17 CFR 249.220f.

42 A number of past Commission releases provide general interpretive guidance on these disclosure requirements. See, e.g., Commission Guidance Regarding Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8350 (Dec. 19, 2003) [68 FR 75056 (Dec. 29, 2003)]; Commission Statement About Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 338056 (Jan. 22, 2002) [67 FR 3746 (Jan. 25, 2002)]; Management's Discussion and Analysis of Financial Condition and Results of Operations; Certain Investment Company Disclosures, Release No. 33-6835 (May 18, 1989) [54 FR 22427 (May 24, 1989)].

43 17 CFR 229.303(a).

44 17 CFR 229.101; 17 CFR 249.220f.

cidents or risks materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions, the company must provide appropriate disclosure.

5. Legal Proceedings

Item 103 of Regulation S-K requires companies to disclose information relating to material pending legal proceedings to which they or their subsidiaries are a party.[45] Companies should note that this requirement includes any such proceedings that relate to cybersecurity issues. For example, if a company experiences a cybersecurity incident involving the theft of customer information and the incident results in material litigation by customers against the company, the company should describe the litigation, including the name of the court in which the proceedings are pending, the date the proceedings are instituted, the principal parties thereto, a description of the factual basis alleged to underlie the litigation, and the relief sought.

6. Financial Statement Disclosures

Cybersecurity incidents and the risks that result therefrom may affect a company's financial statements. For example, cybersecurity incidents may result in:

- expenses related to investigation, breach notification, remediation and litigation, including the costs of legal and other professional services;
- loss of revenue, providing customers with incentives or a loss of customer relationship assets value;
- claims related to warranties, breach of contract, product recall/replacement, indemnification of counterparties, and insurance premium increases; and
- diminished future cash flows, impairment of intellectual, intangible or other assets; recognition of liabilities; or increased financing costs.

The Commission expects that a company's financial reporting and control systems would be designed to provide reasonable assurance that information about the range and magnitude of the financial impacts of a cybersecurity incident would be incorporated into its financial statements on a timely basis as the information becomes available.[46]

---

45 17 CFR 229.103.

46 See Section 13(b)(2)(B) of the Exchange Act [15 U.S.C.78m(b)(2)(B)].

7. Board Risk Oversight

Item 407(h) of Regulation S-K and Item 7 of Schedule 14A require a company to disclose the extent of its board of directors' role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board's leadership structure.[47] The Commission has previously said that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company."[48] A company must include a description of how the board administers its risk oversight function.[49] To the extent cybersecurity risks are material to a company's business, we believe this discussion should include the nature of the board's role in overseeing the management of that risk.

In addition, we believe disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area.

B. Policies and Procedures

1. Disclosure Controls and Procedures

Cybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with the federal securities laws. We encourage companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure. Companies should assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and other corporate insiders from trading on the basis of material nonpublic information about cybersecurity risks and incidents.[50]

47 17 CFR 229.407(h); 17 CFR 240.14a-101 – Schedule 14A.

48 Final Rule: Proxy Disclosure Enhancements, Release No. 33-9089 (Dec. 16, 2009) [74 FR 68334 (Dec. 23, 2009)], available at http://www.sec.gov/rules/final/2009/33-9089.pdf.

49 See Item 407(h) of Regulation S-K [17 CFR 229.407(h)].

50 See Final Rule: Certification of Disclosure in Companies' Quarterly and Annual Reports, Release No. 33-8124 (Aug. 28, 2002) [67 FR 57276 (Sept. 9, 2002)], available at https://www.sec.gov/rules/final/33-8124.htm ("We believe that, to assist principal executive and financial officers in the discharge of their responsibilities in making the required certifica-

Pursuant to Exchange Act Rules 13a-15 and 15d-15, companies must maintain disclosure controls and procedures, and management must evaluate their effectiveness.[51] These rules define "disclosure controls and procedures" as those controls and other procedures designed to ensure that information required to be disclosed by the company in the reports that it files or submits under the Exchange Act is (1) "recorded, processed, summarized and reported, within the time periods specified in the Commission's rules and forms," and (2) "accumulated and communicated to the company's management ... as appropriate to allow timely decisions regarding required disclosure."[52]

A company's disclosure controls and procedures should not be limited to disclosure specifically required, but should also ensure timely collection and evaluation of information potentially subject to required disclosure, or relevant to an assessment of the need to disclose developments and risks that pertain to the company's businesses.[53] Information also must be evaluated in the context of the disclosure requirement of Exchange Act Rule 12b-20.[54] When designing and evaluating disclosure controls and procedures, companies should consider whether such controls and procedures will appropriately record, process, summarize, and report the information related to cybersecurity risks and incidents that is required to be disclosed in filings. Controls and procedures should enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents.

Exchange Act Rules 13a-14 and 15d-14[55] require a company's principal executive officer and principal financial officer to make certifications regarding the design and effectiveness of disclosure controls and

---

tions, as well as to discharge their responsibilities in providing accurate and complete information to security holders, it is necessary for companies to ensure that their internal communications and other procedures operate so that important information flows to the appropriate collection and disclosure points in a timely manner."); see also Section 10(b) of the Exchange Act and Rule 10b-5 thereunder [15 U.S.C. 78j(b); 17 CFR 240.10b-5].

51 17 CFR 240.13a-15; 17 CFR 240.15d-15.

52 Id.

53 See Final Rule: Certification of Disclosure in Companies' Quarterly and Annual Reports, Release No. 33-8124 (Aug. 28, 2002) [67 FR 57276 (Sept. 9, 2002)], available at https://www.sec.gov/rules/final/33-8124.htm ("We believe that the new rules will help to ensure that an issuer's systems grow and evolve with its business and are capable of producing Exchange Act reports that are timely, accurate and reliable.").

54 17 CFR 240.12b-20.

55 7 CFR 240.13a-14; 17 CFR 240.15d-14.

procedures,[56] and Item 307 of Regulation S-K and Item 15(a) of Exchange Act Form 20-F require companies to disclose conclusions on the effectiveness of disclosure controls and procedures.[57] These certifications and disclosures should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact. In addition, to the extent cybersecurity risks or incidents pose a risk to a company's ability to record, process, summarize, and report information that is required to be disclosed in filings, management should consider whether there are deficiencies in disclosure controls and procedures that would render them ineffective.

2. Insider Trading

Companies and their directors, officers, and other corporate insiders should be mindful of complying with the laws related to insider trading in connection with information about cybersecurity risks and incidents, including vulnerabilities and breaches.[58] It is illegal to trade a security "on the basis of material nonpublic information about that security or issuer, in breach of a duty of trust or confidence that is owed directly, indirectly, or derivatively, to the issuer of that security or the shareholders of that issuer, or to any other person who is the source of the material nonpublic information."[59] As noted above, information about a company's cybersecurity risks and incidents may be material nonpublic information, and directors, officers, and other corporate insiders would violate the antifraud provisions if they trade the company's securities in breach of their duty of trust or confidence while in possession of that material nonpublic information.[60]

Beyond the antifraud provisions of the federal securities laws, companies and their directors, officers, and other corporate insiders must comply with all other applicable insider trading related rules. Many exchanges require listed companies to adopt codes of conduct and policies that promote compliance with applicable laws, rules, and regulations, including those prohibiting insider trading.[61] We encourage companies to

---

56 Section 302 of the Sarbanes-Oxley Act of 2002 required the Commission to adopt final rules under which the principal executive officer or officers and the principal financial officer or officers, or persons providing similar functions, of an issuer each must certify the information contained in the issuer's quarterly and annual reports. Pub. L. 107-204, 116 Stat. 745 (2002).

57 17 CFR 229.307; 17 CFR 249.220f.

58 In addition to promoting full and fair disclosure, the antifraud provisions of the federal securities laws prohibit insider trading, which harms not only individual investors but also the very foundations of our markets by undermining investor confidence in the integrity of those markets. 17 CFR 243.100. Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 FR 51716 (Aug. 24, 2000)].

59 Rule 10b5-1(a) of the Exchange Act [17 CFR 240.10b-5-1(a)].

60 This would not preclude directors, officers, and other corporate insiders from relying on Exchange Act Rule 10b51 if all conditions of that rule are met.

61 See e.g., NYSE Listed Company Manual Section 303A.10, which states in relevant part that every NYSE "listed com-

consider how their codes of ethics[62] and insider trading policies take into account and prevent trading on the basis of material nonpublic information related to cybersecurity risks and incidents. The Commission believes that it is important to have well designed policies and procedures to prevent trading on the basis of all types of material non-public information, including information relating to cybersecurity risks and incidents.

In addition, while companies are investigating and assessing significant cybersecurity incidents, and determining the underlying facts, ramifications and materiality of these incidents, they should consider whether and when it may be appropriate to implement restrictions on insider trading in their securities. Company insider trading policies and procedures that include prophylactic measures can protect against directors, officers, and other corporate insiders trading on the basis of material nonpublic information before public disclosure of the cybersecurity incident. As noted above, we believe that companies would be well served by considering how to avoid the appearance of improper trading during the period following an incident and prior to the dissemination of disclosure.

3. Regulation FD and Selective Disclosure

Companies also may have disclosure obligations under Regulation FD in connection with cybersecurity matters. Under Regulation FD, "when an issuer, or person acting on its behalf, discloses material nonpublic information to certain enumerated persons it must make public disclosure of that information."[63] The Commission adopted Regulation FD owing to concerns about companies making selective disclosure of material nonpublic information to certain persons before making full disclosure of that same information to the general public.[64]

In cases of selective disclosure of material nonpublic information related to cybersecurity, companies should ensure compliance with Regulation FD. Companies and persons acting on their behalf should not selectively disclose material, nonpublic information regarding cybersecurity risks and incidents to Regulation

---

pany should proactively promote compliance with laws, rules and regulations, including insider trading laws.

62 Item 406 of Regulation S-K [17 CFR 229.406].

63 17 CFR 243.100. Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 FR 51716 (Aug. 24, 2000)].

64 Id.

FD enumerated persons[65] before disclosing that same information to the public.[66] We expect companies to have policies and procedures to ensure that any disclosures of material nonpublic information related to cybersecurity risks and incidents are not made selectively, and that any Regulation FD required public disclosure is made simultaneously (in the case of an intentional disclosure as defined in the rule) or promptly (in the case of a non-intentional disclosure) and is otherwise compliant with the requirements of that regulation.[67]

By the Commission.

Dated: February 21, 2018

Brent J. Fields

Secretary

65 Regulation FD applies generally to selective disclosures made to persons outside the issuer who are (1) a broker or dealer or persons associated with a broker or dealer; (2) an investment advisor or persons associated with an investment advisor; (3) an investment company or persons affiliated with an investment company; or (4) a holder of the issuer's securities under circumstances in which it is reasonably foreseeable that the person will trade in the issuer's securities on the basis of the information. 17 CFR 243.100(b)(1).

66 Final Rule: Selective Disclosure and Insider Trading, Release No. 34-43154 (Aug. 15, 2000) [65 FR 51716 (Aug. 24, 2000)].

67 "Under the regulation, the required public disclosure may be made by filing or furnishing a Form 8-K, or by another method or combination of methods that is reasonably designed to effect broad, non-exclusionary distribution of the information to the public." Id. at 3.

OUR LOCATIONS

ATLANTA
999 Peachtree St., NE, Suite 1000
Atlanta, GA 30309-3915
678.420.9300

BALTIMORE
300 E. Lombard St., 18th Floor
Baltimore, MD 21202-3268
410.528.5600

BOULDER
5480 Valmont Road, Suite 200
Boulder, CO 80301-2369
303.379.2275

DELAWARE
919 N. Market St., 11th Floor
Wilmington, DE 19801-3034
302.252.4465

DENVER
1225 17th St., Suite 2300
Denver, CO 80202-5596
303.292.2400

LAS VEGAS
One Summerlin
1980 Festival Plaza Drive, Suite 900
Las Vegas, NV 89135-2658
702.471.7000

LOS ANGELES
2029 Century Park E., Suite 800
Los Angeles, CA 90067-2909
424.204.4400

MINNEAPOLIS
2000 IDS Center
80 South 8th St.
Minneapolis, MN 55402-2113
612.371.3211

NEW JERSEY
210 Lake Drive E., Suite 200
Cherry Hill, NJ 08002-1163
856.761.3400

NEW YORK
1675 Broadway, 19th Floor
New York, NY 10019-5820
212.223.0200

PHILADELPHIA
1735 Market St., 51st Floor
Philadelphia, PA 19103-7599
215.665.8500

PHOENIX
1 E. Washington St., Suite 2300
Phoenix, AZ 85004-2555
602.798.5400

SALT LAKE CITY
One Utah Center, Suite 800
201 S. Main St.
Salt Lake City, UT 84111-2221
801.531.3000

SIOUX FALLS
101 South Reid St., Suite 302
Sioux Falls, SD 57103
605.978.5200

WASHINGTON, DC
1909 K St., NW, 12th Floor
Washington, DC 20006-1157
202.661.2200

Ballard Spahr LLP

www.ballardspahr.com