Committee).

[26]*See* Alma Cohen, Robert J. Jackson, Jr., & Joshua Mitts, *The 8-K Trading Gap* (August 1, 2016), *available at* https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2657877.

[27]Sophisticated observers wonder how our current law applies to these cases, illustrating the inadequacy of current rules for dealing with cases like this—and our failure to make the rules of the road clear to corporate insiders. *See* Matt Levine, *Money Stuff*, Bloomberg View (March 15, 2018) ("[I]f you work at a public company, and it suffers a massive data breach, and you *don't* find out about it before it is public, and you sell your stock because you just have a vague bad feeling about things, is *that* illegal insider trading? . . .[T]here are some nuances to the question, but the basic answer is no, probably not.").

[28]*See* Mitts & Talley, *supra* note 19 (arguing that, although the "efficiency implications of cybersecurity trading are distinct—and generally more concerning—than those posed by garden-variety information trading within securities markets," "both securities fraud and computer fraud in their current form appear poorly adapted to address such concerns, and both would require nontrivial re-imagining to meet the challenge"); *see also* Matt Levine, *Is Cyber-Insider Trading Illegal?*, Bloomberg View (Feb. 2, 2018) (discussing the study and inquiring, more generally, whether trading of this kind is prohibited by current law).

[29]*See* Marsh, *supra* note 8, at 7 & fig. 4.

[30]Securities and Exchange Commission, *supra* note 8, at 26-27.

[31]Jason Krause, *Does Learning to Code Make You a Better Lawyer?* ABA Journal (Sept. 2016), *available at* http://www.abajournal.com/magazine/article/lawyer_learning_code_zvenyach_ohm.

[32]*See* Twentieth Century Fox, Office Space (1999) (providing the canonical example of justifying one's employment with the claim: "I have people skills.").

[33]That's actually economics, I know. Or is it? *See* Derek Thompson, *Why Economics is Really Called 'the Dismal Science,"* The Atlantic (Dec. 17, 2013) (questioning the standard tale that Thomas Carlyle coined this term in response to Malthus's famous claim that population growth would always strain natural resources).

[34]Marsh, *supra* note 8, at 8.

[35]*See id.* at 8 & fig. 5.

SEC/SRO UPDATE: SEC ISSUES UPDATED CYBERSECURITY GUIDANCE TO PUBLIC COMPANIES; SEC SETTLES FOUR AUDITING CASES WITH ACCOUNTING FIRMS; NYSE AND AFFILIATED EXCHANGES PAY $14 MILLION PENALTY FOR MULTIPLE VIOLATIONS OF REGULATION SCI

By Peter H. Schwartz & Scott Turbeville

Peter H. Schwartz is a partner and Scott Turbeville is an associate in the law firm of Davis Graham & Stubbs LLP in Denver, Colo. The authors thank Sandra Wainer, a paralegal at Davis Graham, for her assistance in preparing this article.
Contact: peter.schwartz@dgslaw.com or scott.turbeville@dgslaw.com.

SEC Issues Updated Cybersecurity Guidance to Public Companies

On February 21, the Securities and Exchange Commission (SEC) issued an interpretive release concerning cybersecurity matters that updated guidance on public company disclosure and other obligations (the Guidance). The SEC Expressed that in its view, investors should be informed in a timely manner about material cybersecurity risks and incidents especially "in light of the increasing significance of cybersecurity incidents."[1]

The interpretive release, entitled "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," reinforces and expands the SEC's Division of Corporation Finance's 2011 CF Disclosure Guidance: Topic No. 2, Cybersecurity,[2] addressing two topics not developed in the 2011 guidance:

- the importance of cybersecurity policies and procedures; and
- the application of insider trading prohibitions in the cybersecurity context.

Disclosure Considerations

The Guidance states that a company should consider the materiality of cybersecurity risks and incidents when preparing its registration statements and periodic and current reports. The Guidance highlights some specific areas of disclosure where companies should pay special attention, and enumerates issues to consider for each area, including:

- the risk factor disclosure required pursuant to Item 503(c) of Regulation S-K and Item 3.D of Form 20-F;
- management's discussion and analysis (MD&A) of financial condition and results of operations required pursuant to Item 303 of Regulation S-K and Item 5 of Form 20-F;
- the discussion of a company's products, services, relationships, and competitive conditions required pursuant to Item 101 of Regulation S-K and Item 4.B of Form 20-F;
- legal proceedings disclosure required pursuant to Item 103 of Regulation S-K;
- financial statement disclosures; and
- the Board's risk oversight disclosure required pursuant to Item 407(h) of Regulation S-K and Item 7 of Schedule 14A.

Beyond requirements explicitly found in regulations, the Guidance notes that companies are also required to disclose material information and revisit or refresh past disclosures, especially during a cybersecurity investigation, as may be necessary to ensure a company's filings are not misleading. In determining disclosure obligations regarding cybersecurity risks and incidents, companies should weigh, among other things, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and the impact of the incident on such company's operations. The Guidance emphasizes that the disclosure should be specifically tailored to a company's risks and incidents, avoiding boilerplate language and generic cybersecurity-related disclosure.

While detailed disclosure is required, the Guidance cautions that it is not intended to suggest that a company make finely detailed disclosures that could provide a "roadmap" for those who seek to penetrate a company's security protections.

Policies and Procedures

The Guidance also encourages companies to adopt comprehensive policies and procedures designed to ensure that the personnel who are responsible for evaluating disclosures within a company are notified of any information related to cybersecurity risks and incidents in a timely manner. In the SEC's view, disclosure controls and procedures should not be limited to solely focus on specifically required disclosure and should be structured to collect and evaluate information in a timely way that could be subject to required disclosure or that could be relevant to an assessment regarding whether a need exists to provide disclosure.

In addition, the Guidance states that 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."

The Guidance encourages companies to have policies and procedures in place to prevent trading on the basis of all types of material nonpublic information, including cybersecurity risks and incidents. Because some cybersecurity risks and incidents may involve

material nonpublic information, "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." When a company is investigating such an incident and assessing its materiality and ramifications, the Guidance advises that consideration should be given as to whether it may be appropriate to implement restrictions on insider trading.

The Guidance also cautions companies and those persons acting on a company's behalf to comply with Regulation FD and not make selective disclosures of material nonpublic information regarding cybersecurity risks and incidents until such information has been publicly disseminated. The SEC expects that companies have policies and procedures in place to ensure selective disclosures are not made and that any Regulation FD-required public disclosure be made either simultaneously (in the case of intentional disclosures) or promptly (in the case of non-intentional disclosures).

SEC Settles Four Auditing Cases with Accounting Firms

On March 13, the SEC announced that it had charged foreign affiliates of three major accounting firms—KPMG, Deloitte & Touche, and BDO—for conducting audits that allegedly circumvented the full oversight of the Public Company Accounting Oversight Board (PCAOB).[3]

According to the SEC, the Zimbabwe affiliates of Deloitte & Touche and KPMG improperly audited the majority of assets and revenues of a publicly traded company without registering with the PCAOB. The company's two principal auditors—KPMG's affiliate in South Africa and BDO's affiliate in Canada—were registered with the PCAOB but improperly relied upon the work of the two unregistered Zimbabwe affiliates to complete their audits, violating PCAOB standards.

The firms agreed to settle the charges by paying penalties and disgorging their profits from the audits, as applicable.

NYSE and Affiliated Exchange Pay $14 Million Penalty for Multiple Violations of Regulation SCI

On March 6, the SEC announced that it charged the New York Stock Exchange (NYSE), and two affiliated exchanges—NYSE Arca and NYSE American—with regulatory failures involving multiple events, including several disruptive market events.[4] The charges arose from five separate investigations and included the first-ever charged violation of Regulation SCI's business continuity and disaster recovery requirement.

Regulation SCI was adopted by the SEC in 2014 with the goal of seeking to strengthen the technology infrastructure and integrity of the U.S. securities markets.[5]

According to the SEC's order, the violations included "erroneously implementing a market-wide regulatory halt, negligently misrepresenting stock prices as 'automated' despite extensive system issues ahead of a total shutdown of two of the exchanges, and applying price collars during unusual market volatility on Aug. 24, 2015, without a rule in effect to permit them"—which the SEC alleged caused the market imbalances to be resolved more slowly than they would have been had those actions not occurred.

The SEC's order also found, among other things, that the NYSE exchanges broke rules regarding business continuity and disaster recovery in violation of Regulation SCI and violated Regulation NMS.

The exchanges neither admitted nor denied the findings in the SEC's order and, in settlement, agreed to pay a $14 million penalty.

ENDNOTES:

[1]*See* "Commission Statement and Guidance on Public Company Cybersecurity Disclosures" (Feb. 21, 2018), *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf.

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

[3]*See* SEC Rel. No. 2018-39 (Mar. 13, 2018), *available at* https://www.sec.gov/news/press-release/2018-39. *See also* SEC Lit. Rel. No. 34-82859 (Mar. 13, 2018), *available at* https://www.sec.gov/litigation/admin/2018/34-82859.pdf (order - BDO Canada LLP); SEC Lit. Rel. No. 34-82859 (Mar. 13, 2018), *available at* https://www.sec.gov/litigation/admin/2018/34-82860.pdf (order - KPMG Inc.); SEC Lit. Rel. No. 34-82861 (Mar. 13, 2018), *available at* https://www.sec.gov/litigation/admin/2018/34-82861.pdf (order - Deloitte and Touche Chartered Accountants); and SEC Lit. Rel. No. 34-82862 (Mar. 13, 2018), *available at* https://www.sec.gov/litigation/admin/2018/34-82862.pdf (order - KPMG).

[4]*See* SEC Rel. No. 2018-31 (Mar. 6, 2018), *available at* https://www.sec.gov/news/press-release/2018-31 . *See also* SEC Lit. Rel. No. 33-10463 (Mar. 6, 2018), *available at* https://www.sec.gov/litigation/admin/2018/33-10463.pdf (order).

[5]*See* Regulation Systems Compliance and Integrity, Final Rule Release, 79 Fed. Reg. 72252 (Dec. 5, 2014).