35 MILLION REASONS TO HEED NEW SEC GUIDANCE ON CYBERSECURITY DISCLOSURE REQUIREMENTS

By John McCauley Esq., CIPP (US)(E) Bingham Greenebaum Doll LLP

The Securities and Exchange Commission has released new guidance ("Guidance") to ensure public companies disclose cybersecurity incidents and risks to their investors. As evidence of its view of the importance of the Guidance, the SEC in April 2018 announced a $35 million settlement with Altaba, (formerly Yahoo), which waited two years to disclose a massive data breach in 2014.

In February 2018, the Securities and Exchange Commission ("Commission") approved Interpretive Guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents. The decision vote to approve the Guidance comes at a time when the significance of cybersecurity incidents is increasing.

The Guidance outlines the Commission's views with respect to cybersecurity disclosure requirements under the federal securities laws as they apply to public operating companies.

WHY GIVE GUIDANCE?

After the issuance of Guidance in 2011, the SEC found many companies included additional cybersecurity disclosure, typically in the form of risk factors. However, given the frequency, magnitude and costs associated with cybersecurity incidents to public companies, the SEC believes companies must take all required actions to inform investors about a material cybersecurity risk or incident in a timely manner. Companies that are the victim of a cyberattack or other cybersecurity incident often incur substantial costs, including remediation costs, increased cybersecurity protection costs, reputational harm, and litigation and legal risks, including regulatory actions by governmental authorities.

It is important to note that the Guidance outlined regarding disclosure also applies to companies that have not yet had an incident but may be at risk for a cyberattack.

The Commission's Interpretive Guidance focuses on two areas that were not addressed in the Division of Finance's Guidance – 1) the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents; and 2) the application of insider trading prohibitions in the cybersecurity context.

POLICIES AND PROCEDURES

The SEC expects companies to disclose any cybersecurity risk or incident that is material to investors, including the concomitant financial, legal or reputational consequences. Companies will have to weigh the potential materiality of any identified risk, the importance of any compromised information and the impact of the incident on the company's operations. Companies should also avoid a generic approach to completing the disclosure forms and provide specific information that is useful to investors.

But this does not mean companies are to give a roadmap regarding their security plans, such as technical information about their cybersecurity efforts or other details that will make the company and its technology more susceptible to an incident.

Companies have a duty to correct prior disclosures that the company later determines were untrue at the time they were made. Companies should consider whether they need to revisit or refresh any previous disclosures, including during the process of investigating a cybersecurity incident, in light of this new Guidance.

In addition, the SEC encourages companies to adopt comprehensive policies and procedures related to cybersecurity disclosure. Compliance with these policies and procedures should be evaluated regularly.

INSIDER TRADING

Companies and their directors, officers and other corporate insiders are obligated to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents. They must 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 SEC notes it is continuing to monitor cybersecurity disclosures carefully.

In fact, in March 2018, the federal government filed criminal and civil charges against Jun Ying, a former chief information officer at Equifax Inc., over alleged insider trading linked to Equifax's massive data breach in 2017. He is accused of using confidential information to conclude the company suffered a serious breach, and then sold his shares of the company before the breach was announced, making nearly $1 million.

By selling before the data breach was publicly disclosed, he avoided nearly $117,000 in losses, according to the SEC. It is the first time the U.S. government has charged someone with insider trading after allegedly profiting from information about a cyberattack.

The Commission encourages companies to consider how their codes of ethics and insider trading policies take into account and prevent trading on the basis of material nonpublic information related to a cybersecurity risk or incident. It is prudent for companies to consider how to avoid the appearance of improper trading during the period following a cybersecurity incident and before information about the disclosure is disseminated.

TAKE ACTION

On April 24, 2018, the SEC announced the $35 million settlement with Altaba to resolve the Commission's charges that Yahoo deceived investors by not disclosing a massive data breach in December 2014 to the investing public until 2016 when it was in the process of closing the acquisition of its operating business by Verizon Communications, Inc. Yahoo neither admitted nor denied the findings in the SEC's order.

The message from the SEC is clear – the Division of Finance will continue to carefully monitor cybersecurity disclosures as part of its selective filing reviews. Public companies should work with their legal and compliance teams to evaluate their controls and procedures regarding securities law disclosure obligations and how to avoid the appearance of improper insider trading during the time after a cybersecurity incident but before that information has been included in a disclosure.

Bingham Greenebaum Doll LLP Partner John McCauley provides extensive advice on cybersecurity risks, incidents and policy issues, including proactive cyber incident readiness. As a Certified Information Privacy Professional, he assists clients in identifying, evaluating and managing risks associated with privacy and information security practices.