Kevane Grant Thornton

An instinct for growth™

Audit

Computer

Guidance

New interpretive guidance on cybersecurity disclosures

April 19, 2018

Aida Ramirez
Partner Head of Audit
Kevane Grant Thornton
T (1) 787 754 1915
E aida.ramirez@pr.gt.com

Access our Professional Articles on:
www.grantthornton.pr

On February 20, the Security and Exchange Commission approved an Interpretive Release, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, to provide guidance to public operating companies when preparing disclosures about cybersecurity risks and incidents. The release does not apply to other regulated entities under the federal securities laws, such as registered investment companies, investment advisers, brokers, dealers, exchanges, and self-regulatory organizations.

The interpretive guidance reinforces and expands upon the Division of Corporation Finance (CorpFin) staff's Disclosure Guidance, Topic No. 2: "Cybersecurity, issued in 2011. The Commission addresses two new topics in its release, stressing the importance of companies' cybersecurity policies and procedures around the timely disclosure of cybersecurity risks and incidents, as well as the application of insider trading prohibitions within the cybersecurity context. More specifically, the release notes the following guidance:

- disclosure controls and procedures: Companies are required to establish and maintain appropriate and effective disclosure controls and procedures that enable them to accurately and timely disclose material events, including those related to cybersecurity. The guidance encourages companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly. Also, companies should ensure that the disclosure controls and procedures are sufficient enough to escalate the relevant information to appropriate personnel when cybersecurity risks and incidents do exist.
- in addition, management should consider whether there are deficiencies in disclosure controls and procedures that would render them ineffective to the extent that

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.
- insider trading: companies are encouraged 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 cybersecurity risks and incidents.
- Regulation FD and selective disclosure: companies should make timely disclosures of material, nonpublic information regarding cybersecurity risks and incidents, and refrain from making selective disclosures to ensure compliance with Regulation FD.

The interpretive guidance also addresses the Commission's views and expectations regarding specific disclosure of cybersecurity risks and incidents under the federal securities laws, as follows:

- *materiality:* companies should provide timely and ongoing disclosures that are material and useful to investors, while avoiding boilerplate disclosures.
- *risk factors:* companies should include relevant cybersecurity risks if those risks make investments in the company's securities speculative or risky, including risks that arise in connection with acquisitions. Companies should also consider previous or ongoing cybersecurity incidents to provide the appropriate context within the risk factor disclosure.
- *management's discussion and analysis of financial condition and results of operations:* companies should include relevant discussion around the array of costs associated with cybersecurity issues, including costs of ongoing efforts and other consequences of incidents, if these costs are reasonably likely to have a material effect on the company's results of operations, liquidity, or financial condition. Companies are expected to assess the impact of any incidents on reportable segments as well.
- *description of business:* companies should provide appropriate disclosure if cybersecurity incidents or risks materially affect a company's products, services, relationship with customer or suppliers, or competitive conditions.
- *legal proceedings:* companies should disclose information relating to material pending legal proceedings that relate to cybersecurity issues.
- *financial statement disclosures:* companies should maintain financial reporting and control systems that are designed to provide information about the range and magnitude of the financial impact of a cybersecurity incident on a timely basis as the information becomes available.
- *board risk oversight:* companies should disclose the board of director's involvement in the oversight of the risk management process related to cybersecurity risks, to the extent they are material to a company's business.

In a statement on February 21, SEC Chairman Jay Clayton remarked that he has asked CorpFin to continue to monitor cybersecurity disclosures as part of their selective filing reviews, and that the SEC will continue to evaluate developments and consider feedback about whether any further guidance or rules are needed.

The interpretive release became effective February 26.

Source:
Grant Thornton, On the Horizon, March 1, 2018.

We are committed to keep you updated of all developments that may affect the way you do business in Puerto Rico. Please contact us for further assistance in relation to this or any other matter.

Kevane Grant Thornton
An instinct for growth™

grantthornton.pr