SEC Investigative Report Underscores Importance of Internal Accounting Controls to Protect Against Cyber-Scams

I. Overview

On October 16, 2018, the Securities and Exchange Commission (the "Commission") issued an investigative report under Section 21(a) of the Securities Exchange Act of 1934 (the "Report") signaling that public companies may need to enhance internal accounting controls to prevent and mitigate cyber-related risks and to ensure compliance with the federal securities laws.[1] The Commission issued the Report following an enforcement investigation into whether nine companies violated the securities laws by failing to maintain sufficient internal accounting controls to prevent cyber-scams. The investigation focused on companies that have fallen victim to a type of scam referred to as a "business email compromise" (or "BEC"). In the BECs under investigation, bad actors send hoax e-mails posing as company executives or vendors requesting payments. The consequences of these events can be significant for their victims, and the BECs under investigation resulted in collective losses of nearly $100 million. Although the Commission ultimately did not pursue enforcement actions against the investigated companies, the Report puts public companies on notice that "internal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds."[2]

II. The Report

The Commission issues reports of investigation under Section 21(a) of the Exchange Act when it wishes to publicize investigative findings without filing an enforcement action. The reports are generally understood to be statements of Commission policy. Here, the Report focuses on the importance of accounting controls in preventing and mitigating cyber-risks. The Report also alerts companies that they may be the subject of an enforcement action if their accounting controls are insufficient.

The Commission's investigation focused on two related cyber-scams:

- ***E-mails from Purported Executives*:** Bad actors send e-mails to personnel within a company's finance department using a spoofed e-mail domain, purporting to be a company executive directing them to wire large sums of money to a foreign bank account, typically in a short period of time. The Report characterizes these schemes as relatively unsophisticated from a technological standpoint, requiring only a fake domain name.

- ***E-mails from Purported Vendors*:** Bad actors hack the e-mail accounts of a company's foreign vendors and send invoices and payment requests to the company for otherwise legitimate transactions. The Report points out that this scheme was particularly difficult to detect; some companies only become aware that they have been the victims of a fraud when the real vendors inquire about delinquent bills.

[1] *See* SEC, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements (Oct. 16, 2018), *available at* https://www.sec.gov/litigation/investreport/34-84429.pdf.

[2] *Id.* at 6.

The Report explains that these two schemes "underscore the importance of devising and maintaining a system of internal accounting controls attuned to this kind of cyber-related fraud, as well as the critical role training plays in implementing controls that serve their purpose and protect assets in compliance with the federal securities laws."[3] The Report also warns that frauds stand a high chance of success when the responsible personnel fail to understand and implement a company's existing controls or fail to recognize red flags.

III. Next Steps

Given the increasing likelihood of regulatory scrutiny—not to mention the greatly increasing risks of loss—it is important for companies to review their internal accounting controls and policies and procedures to ensure that they are updated to address the developing cyber-risk landscape. The Report acknowledges that not every "victim of a cyber-related scam is, by extension, in violation of the internal accounting controls requirements of the federal securities laws."[4] Nonetheless, companies should view the Report as a warning that if they fall victim to cyber-scams, then the company and its leadership may be subjected to a Commission enforcement action. The Commission has focused increasingly on cybersecurity issues, particularly with regard to the intersection of (i) disclosure of cyber-breaches or incidents and (ii) disclosure controls.[5]

In consultation with their outside counsel, companies should consider implementing or revisiting the following controls:

- ***Training*:** Conduct regular employee training on "phishing" and other cyber-scams and BECs, particularly for employees in the finance department, and document both the participation and training content.

- ***Governance*:** Designate responsibility and reporting lines for cybersecurity threats, training and preparedness including both executives and directors; designate a chief security officer.

- ***Configure an External E-mail Recipient Warning*:** Consider adding a warning badge (*e.g.*, "External") to e-mails received from external domains to notify employees and help reduce the likelihood of success of spoofing scams.

- ***Limit Authority and Add Controls to Approve/Change Certain Wire Transactions*:** To the extent possible, limit the employees who have the authority to approve or change significant wire transactions. Consider adding two-step authentication for certain wire transactions.

[3] *Id.* at 5.

[4] *Id.* at 6.

[5] *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018), *available at* http://sec.gov/rules/interp/2018/33-10459.pdf; *see also* Jay Clayton, SEC Chairman, Statement on Cybersecurity Interpretative Guidance (Feb. 21, 2018), *available at* https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21 ("Public companies must stay focused on [cybersecurity] issues and take all required action to inform investors about material cybersecurity risks and incidents in a timely fashion."); *see e.g.*, SEC Press Release, Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million (Apr. 24, 2018), *available at* https://www.sec.gov/news/press-release/2018-71 (agreeing to pay a $35 million penalty to settle charges that it misled investors by failing to disclose one of the world's largest data breaches in which hackers stole personal data relating to hundreds of millions of user accounts).

- ***Phishing Campaign*:** Consider conducting a "white-hat" phishing campaign to assess whether employees are complying with internal accounting controls and policies.

The Report is an important reminder that, in addition to meeting their disclosure obligations, companies must use appropriate tools at their disposal to counteract cyber-scams, including by "calibrat[ing] their internal accounting controls to the current risk environment and assess[ing] and adjust[ing] policies and procedures accordingly."[6]

* * *

If you have any questions about the issues addressed in this memorandum, or if you would like a copy of any of the materials mentioned in it, please do not hesitate to call or email Bradley J. Bondi at 202.862.8910 or bbondi@cahill.com; David R. Owen at 212.701.3955 or dowen@cahill.com; C. Wallace Dewitt at 202.862.8932 or cwdewitt@cahill.com; Matthew M. McDonagh at 212.701.3959 or mmcdonagh@cahill.com; Charles A. Gilman at 212.701.3403 or cgilman@cahill.com; Helene R. Banks at 212.701.3439 or hbanks@cahill.com; or Geoffrey E. Liebmann at 212.701.3313 or gliebmann@cahill.com.

[6] SEC, *supra* note 1, at 6.

This memorandum is for general information purposes only and is not intended to advertise our services, solicit clients or represent our legal advice.