October 29, 2018

SEC Issues Report Reminding Registrants to Consider Cyber Threats When Implementing Internal Accounting Controls

On October 16, 2018, the Securities and Exchange Commission (the "SEC") issued a Report of Investigation ("Report") (available here) cautioning public companies to carefully consider cyber threats when implementing and maintaining their internal accounting controls. The Report is based on the Enforcement Division's investigations of nine SEC registrants spanning multiple industries that were victims of cyber fraud. Although the SEC declined to take enforcement action, it noted that public company internal accounting controls may need to be reassessed in light of risks from increasingly widespread cyber-related frauds.

The Report highlights the SEC's increased focus on cybersecurity issues following its release of guidance in February 2018 to assist registrants in preparing disclosures concerning cybersecurity risks and incidents. The guidance, discussed in our earlier client alert, reminded registrants to assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity issues is processed and reported to the appropriate personnel to enable senior management to make decisions about public disclosure and fulfill their certification obligations. Shortly following the release of that guidance, the company formerly known as Yahoo! was fined $35 million to settle charges that it misled investors by failing to disclose a significant data breach (see our client alert here).

Following the release of the Report, the SEC will likely also apply increased scrutiny to the adequacy of registrants' internal accounting controls with respect to cybersecurity risks.

Cyber-Related Frauds Investigated

The Enforcement Division's investigations focused on "business email compromises" (or "BECs"), in which perpetrators pose as company executives or vendors and use emails to fraudulently induce company employees to send large sums to foreign bank accounts. Each of the registrants investigated lost at least $1 million; two lost more than $30 million, and one lost more than $45 million. In total, the nine registrants wired nearly $100 million as a result of the fraudulent emails, most of which was unrecoverable.

In connection with the investigations, the SEC considered whether the registrants complied with the requirements of Sections 13(b)(2)(B)(i) and (iii) of the Securities Exchange Act of 1934 (the "Exchange Act"). Those provisions require registrants to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that transactions are executed with, or that access to company assets is permitted only with, management's general or specific authorization.

The investigation focused on two variants of schemes involving spoofed or compromised electronic communications from persons purporting to be company executives or vendors.

- ***Emails from Fake Executives***. The first type of cyber-related fraud involved emails purporting to be from company executives. The perpetrators emailed company finance personnel, using spoofed email domains and addresses of an executive (typically the CEO) so that it appeared, at least superficially, as if the email were legitimate. In all of the frauds, the spoofed email directed the registrants' finance personnel to work with a purported outside attorney identified in the email, who then directed the registrants' finance personnel to initiate wire transfers to foreign bank accounts controlled by the perpetrators. The perpetrators used real law firm and attorney names, and legal services-sounding email domains like "consultant.com," but the contact details connected company personnel with an impersonator and co-conspirator. As noted in the Report, these were not sophisticated frauds in general design or the use of technology and only required creating an email address to mimic the executive's address.

- ***Email from Fake Vendors***. The second type of cyber-related fraud involved emails impersonating the registrants' vendors. This form of fraud was more technologically sophisticated than the spoofed executive emails because, in the instances the Division reviewed, the schemes involved intrusions into the email accounts of registrants' foreign vendors. After hacking the existing vendors' email accounts, the perpetrators inserted illegitimate requests for payments into electronic communications for otherwise legitimate transaction requests and corresponded with unwitting company employees responsible for procuring goods from the vendors, then requested that the employees initiate changes to the vendors' banking information and attached doctored invoices reflecting the new, fraudulent account information. The company employees responsible for procurement relayed that information to accounting personnel responsible for maintaining vendor data. As a result, the registrants made payments on outstanding invoices to foreign accounts controlled by the impersonator rather than the accounts of the real vendors.

Implications for Public Companies' Internal Accounting Controls

In the Report, the SEC noted that in light of the risks associated with expanding digital interconnectedness, registrants should pay particular attention to the obligations imposed by Section 13(b)(2)(B) of the Exchange Act to devise and maintain internal accounting controls that reasonably safeguard company assets from cyber-related frauds. More specifically, Section 13(b)(2)(B)(i) and (iii) require certain registrants to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that (i) transactions are executed in accordance with management's general or specific authorization," and that "(iii) access to assets is permitted only in accordance with management's general or specific authorization."

The SEC further noted that the incidents of cyber-related fraud discussed in the Report underscore the importance of devising and maintaining a system of internal accounting controls attuned to cyber 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. In the context of the BECs the Division reviewed, the frauds succeeded, at least in part, because the responsible personnel did not sufficiently understand their company's existing controls or did not recognize indications in the emailed instructions that those communications were fraudulent. While most of the affected registrants had some form of training regarding controls and information technology in place prior to the scams, all of them enhanced their training of responsible personnel about relevant threats, as well as about pertinent policies and procedures following the cyber-related frauds.

Although the SEC stated in the Report that it is not suggesting that every registrant that is the victim of cyber-related fraud is, by extension, in violation of the internal accounting controls requirements of the federal securities laws, it noted that internal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds, and registrants must calibrate their internal accounting controls to the current risk environment and assess and adjust policies and procedures accordingly. According to the Report, in performing this analysis, registrants should evaluate to what extent they should consider cyber-related threats when devising and maintaining their internal accounting control systems. Given the prevalence and continued expansion of these attacks, registrants should be mindful of the risks that cyber-related frauds pose and consider whether their internal accounting control systems are sufficient to provide reasonable assurances in safeguarding their assets from these risks.

Although no charges were brought against the registrants or their employees in connection with the matters discussed in the Report, the Report should be read as a warning to registrants that future investigations of cyber-related fraud may result in enforcement action if the company's internal accounting controls are found to be insufficient to reasonably safeguard the company's assets from cyber-related fraud.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Mark S. Bergman
+44-20-7367-1601
mbergman@paulweiss.com

Andrew J. Foley
+1-212-373-3078
afoley@paulweiss.com

David S. Huntington
+1-212-373-3124
dhuntington@paulweiss.com

Brian M. Janson
+1-212-373-3588
bjanson@paulweiss.com

John C. Kennedy
+1-212-373-3025
jkennedy@paulweiss.com

Tracey A. Zaccone
+1-212-373-3085
tzaccone@paulweiss.com

Hank Michael
+1-212-373-3892
hmichael@paulweiss.com