Oct. 29, 2018

SEC Cautions That Cyber-Related Fraud Could Evidence Failed Internal Accounting Controls

On Oct. 16, 2018, the Securities and Exchange Commission (the "SEC") released a cautionary **report** discussing whether certain public companies that had become victims of cyber-related fraud may have violated federal securities laws by failing to have adequate internal controls over financial reporting. Companies should take note of the SEC's report and carefully consider if they have implemented the safeguards and training necessary to avoid falling victim to such fraud.

The SEC's report noted the increasing frequency and pervasiveness of cyber-related fraud perpetrated against business and focused on nine public companies that had become victims of a particular type of fraud referred to generally as "business email compromises." It is estimated that such fraud has resulted in over $5 billion in losses since 2015. Each of the nine issuers in the report had lost at least $1 million and, in total, they had lost nearly $100 million. These attacks are relatively simple from a technical perspective but have proven to be effective, in spite of the fact that they are all seemingly preventable.

The common theme to this type of attack is phony email communications that appear to come from company management or vendors of the company. These emails often request that the recipient wire funds to bank accounts controlled by the attackers. Employees acquiesce to such requests because the attackers rely on tactics intended to lend legitimacy to the communications and to create confusion. In some instances, attackers will engage in spoofing, hacking email addresses, and incorporating real names of company management or actual vendors in their emails to trick employees into believing the requests are authentic. The SEC report also highlighted social engineering techniques that attackers use to manufacture a sense of urgency, such as claiming the payments are necessary to close time-sensitive "deals" or to make good on past invoices with vendors. In some of the investigated cases, attackers further claimed that payment was needed for a "secret" transaction or subject to regulatory oversight to discourage employees from discussing the situation or give them a sense of comfort. These tactics encourage compliance with the requests in spite of their unusual nature, lack of context or specificity, and even presence of spelling or grammatical errors in the messages.

Section 13(b)(2)(B) of the Securities Exchange Act of 1934, as amended (the "Exchange Act"), requires public companies with a class of securities registered under Section 12 of the Exchange Act to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that transactions are executed and access to company assets is only granted in accordance with authorization from company management. The SEC emphasized that, although cybersecurity threats are relatively new, the expectation and requirements under the Exchange Act remain the same.

The report echoes other recent statements and guidance from the SEC that cybersecurity threats are a significant problem facing all industries and may implicate federal securities laws. The SEC has previously emphasized that companies should implement adequate internal controls and

cybersecurity risk management policies and procedures to face these threats, and disclose material cybersecurity risks and material breaches to comply with disclosure, antifraud and other obligations under federal securities laws. Even if a company's accounting controls, policies and procedures are adequate on paper, the report noted that employees may either be unfamiliar with or confused by their obligations. For example, in one of the investigated matters, an accounting employee misinterpreted an approval matrix and believed that he had the same authority as the company's chief financial officer to conduct money transfers. In addition, human error always creates risk, particularly as technology opens up more avenues of attack from fraudsters.

Every company is different and there is no "one-size-fits-all" approach to creating a set of controls or a compliance program to protect against fraudsters and cybersecurity incidents. Nevertheless, there are some best practices companies should consider to mitigate the specific threats highlighted in the report. Companies should consider:

- Assigning an individual or team of individuals with proactively reviewing, implementing and monitoring existing policies and controls. Maintaining an adequate security program requires constant vigilance, and it is important that at least one individual is responsible for monitoring new threats and identifying vulnerabilities within the company on an ongoing basis.
- Verifying that existing policies and controls are being effectively implemented. As companies grow and evolve, old policies may no longer be applicable or reflect their current practices.
- Implementing training on these subjects for new employees and all employees on an ongoing basis. Training is one of the most effective tools to combat social engineering and the other types of fraud identified by the SEC. By requiring periodic trainings for all employees, companies can help keep the risk of fraud at the forefront of their employees' minds.
- Updating existing policies and controls to not only address known threats, but to meet other compliance standards that the company may be subject to. It is more efficient to update a single set of policies or controls to both address new risks and move toward compliance with other applicable related laws such as those related to cybersecurity or data privacy rather than to revisit them sporadically or only as needed.

The SEC determined not to pursue any enforcement actions in the investigated matters based on the conduct and activities of the public issuers in question. Instead, the SEC elected to issue a report under Section 21(a) of the Exchange Act to make issuers and market participants aware that cyber-related fraud should be considered when devising and maintaining internal accounting controls as required by federal securities laws. The report noted expressly that the SEC is not suggesting that every issuer that is a victim of cyber-related fraud is in violation of the internal accounting controls requirements of federal securities laws.

If you have questions about the report or cybersecurity and data privacy issues generally, please contact a member of Brownstein's Securities or Cybersecurity and Data Privacy practice groups.

Oct. 29, 2018

Rikard D. Lundberg
Shareholder
rlundberg@bhfs.com
303.223.1232

Ian V. O'Neill
Shareholder
ioneill@bhfs.com
303.223.1210

Esteban M. Morin
Associate
emorin@bhfs.com
303.223.1275

Trayton D. Oakes
Associate
toakes@bhfs.com
303.223.1295