DrinkerBiddle

Client Alert

October 22, 2018

Cyber-Fraud Victim or Securities Law Violator?

By Peter W. Baldwin and Mary P. Hansen

On October 16, 2018, the Securities and Exchange Commission (SEC) released a report detailing its consideration of whether certain companies that had been victims of cyber-related frauds may have violated the federal securities laws by failing to have a sufficient system of internal accounting controls. The issuance of the SEC's report coincides with National Cybersecurity Awareness Month. The SEC issued the report pursuant to its authority under Section 21(a) of the Securities Exchange Act of 1934. The SEC uses its authority under Section 21(a) sparingly and usually when it wants to send a strong warning message about the relevant conduct. When considered along with other recent cybersecurity disclosure guidance by the SEC, the report strongly indicates that cybersecurity is an important SEC enforcement priority.

The SEC's investigation looked at the internal controls of nine companies – from a wide range of industry sectors, including technology, machinery, real estate, energy, financial services and consumer goods – that had been victimized by one of two variants of fraudulent "business email compromise" (BEC) schemes, which involve spoofed or compromised electronic communications. In some of these schemes, perpetrators purporting to be company executives used spoofed email addresses and directed the companies' finance personnel to make large wire transfers to foreign bank accounts. In other instances, the perpetrators impersonated the companies' vendors and requested that the companies initiate changes to the vendors' banking information and then make large wire transfers to the new bank accounts. Each of the companies lost more than $1 million as a result of the BEC schemes, and two lost more than $30 million. The FBI recently estimated that BEC schemes like those described in the SEC's report have caused over $5 billion in losses since 2013 – the highest estimated out-of-pocket losses from any class of cyber-facilitated crime over this period.

The SEC considered whether the companies that were victimized by the BEC schemes had complied with Sections 13(b)(2)(B)(i) and (iii) of the Securities Exchange Act of 1934, which require issuers 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 require that "(iii) access to assets is permitted only in accordance with management's general or specific authorization." Ultimately, the SEC did not pursue an enforcement action against any of the companies that were the subject of the investigations.

Nevertheless, the SEC cautioned that companies subject to the internal accounting controls requirements of Section 13(b)(2)(B) must calibrate their internal accounting controls to the current risk environment and assess and adjust policies and procedures accordingly. Specifically, the SEC advised that issuers must be aware that these cyber-related threats of spoofed or manipulated electronic communications exist and must be considered when devising and maintaining a system of internal accounting controls. This is consistent with the SEC's February 2018 Statement and Guidance on Public Company Cybersecurity Disclosures, which advised companies that "[c]ybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with the federal securities laws."

Public companies of all types are increasingly the targets of sophisticated cyber criminals. In light of the current risk environment, companies must pay careful attention to the obligations imposed by Section 13(b)(2)(B) to devise and maintain internal accounting controls that reasonably protect the company and its investors from cyber-related threats. Having controls that contemplate cyber-related threats will be vital to maintaining a sufficient accounting control environment and safeguarding assets.

Through the release of its report, the SEC has put companies on notice that enforcement actions may be contemplated for companies that are victimized by cyber-related frauds. As such, the report underscores the importance of devising and maintaining a system of internal accounting controls attuned to BECs and related cyber frauds, as well as the critical role that training plays in implementing these controls. Companies should look to enhance their payment authorization procedures and verification requirements for vendor information changes. In addition, companies should examine their account reconciliation procedures and outgoing payment notification processes to ensure that payments resulting from fraud are detected and stopped. Companies must also look to enhance their training of employees about key cyber-related threats, as well as the relevant internal policies and procedures governing issues such as payment authorization and verification.

Finally, it is important to keep in mind that while the cyber threats discussed in the SEC's report related to payment authorization and verification, public issuers should regularly reassess their internal accounting controls in light of all types of cyber-related risks.

White Collar Defense and Corporate Investigations Team

Primary Contacts

Peter. W. Baldwin
Partner

New York
(212) 248-3147
peter.baldwin@dbr.com

Mary P. Hansen
Partner

Philadelphia
(215) 988-3317
mary.hansen@dbr.com