WILMERHALE

SEC Cautions Issuers to Consider Cyber Threats When Devising and Maintaining Internal Accounting Controls

OCTOBER 17, 2018

Yesterday, the Securities and Exchange Commission released an investigative report regarding its investigation into whether nine public companies that were victims of cyber-related frauds violated federal securities laws by failing to have a sufficient system of internal accounting controls. While the SEC determined not to pursue enforcement actions against these issuers with respect to the investigated matters, the report illustrates the importance of considering cyber threats when devising and maintaining internal accounting controls.

The SEC's investigation specifically focused on "business email compromises," which involved fake emails from persons purporting to be company executives or vendors, and examined the internal accounting controls at issuers that fell victim to such schemes. The nine investigated issuers covered a range of sectors, including technology, machinery, real estate, energy, financial, and consumer goods, with each issuer losing at least $1 million and two issuers losing upwards of $30 million. In total, the investigated issuers lost nearly $100 million, most of which was unrecovered. The schemes involving fake emails from company executives involved relatively unsophisticated techniques in terms of the overall design and the technology used. For instance, the scheme essentially involved creating an e-mail address to mimic that of the purported sender. All of the e-mails described a time-sensitive transaction or matter about which minimal information was provided and often included spelling and grammatical errors. The schemes involving emails from fake vendors had fewer indicia of illegitimacy and involved email requests to wire money that originated from hacked email accounts of the issuer's foreign vendors. As the report illustrates, weaknesses in company policies and procedures and human vulnerabilities ultimately contributed to the success of these schemes.

When discussing cyber-related threats, the SEC continues to reemphasize guidance from its February *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (see our February 23, 2018 post). The report quotes the February guidance, noting that "cybersecurity presents ongoing risks and threats to our capital markets and to companies operating in all industries, including public companies regulated by the Commission." The report also makes clear that "[w]hile the cyber-related threats posed to issuers' assets are relatively new, the expectation that issuers will have sufficient internal accounting controls and that those controls

will be reviewed and updated as circumstances warrant is not."

Given the ongoing cyber-related risks that companies face, issuers are encouraged to "pay particular attention to the obligations imposed by Section 13(b)(2)(B) [of the Securities Exchange Act of 1934] to devise and maintain internal accounting controls that reasonably safeguard company and, ultimately, investor assets from cyber-related frauds." Specifically with respect to the schemes involved in the SEC's investigation, "[h]aving internal accounting control systems that factor in such cyber-related threats, and related human vulnerabilities, may be vital to maintaining a sufficient accounting control environment and safeguarding assets." Though "the Commission is not suggesting that every issuer that is the victim of a cyber-related scam is, by extension, in violation of the internal accounting controls requirements . . . , internal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds."

In thinking about their response to the issues raised by this report, companies should consider whether they would benefit from implementing some or all of the remedial measures adopted by the affected companies, which included:

- Clarifying and enhancing payment authorization procedures
- Adopting verification requirements for vendor information changes
- Enhancing account reconciliation and payment verification procedures with vendors to help more quickly identify any fraudulent activity
- Providing additional training to employees about cybersecurity threats and how to avoid common cyber frauds

Authors

Alan J. Wilson

PARTNER

alan.wilson@wilmerhale.com

+1 202 663 6474

Jonathan Wolfman

PARTNER

Co-Chair, Corporate Governance and Disclosure Group

jonathan.wolfman@wilmerhale.com

+1 617 526 6833