Client Alert | Data, Privacy & Cybersecurity / US Public Company Advisory

Stop Payment: SEC Investigative Report Highlights Need for Proper Training, Controls to Prevent Cyber-Related Fraud

October 2018

Authors: Steven R. Chabinsky, Michelle Rutta, Era Anagnosti, Mark Williams

The Securities and Exchange Commission ("SEC") decided not to pursue enforcement actions against any of nine publicly traded companies, each of which lost over $1 million when their internal accounting controls failed to detect fraudulent email requests for wire transfers or vendor payments. The SEC published an investigative report[1] (the "Report") on the incidents to ensure that market participants consider the cyber-related risks of spoofed or manipulated email when devising and maintaining their systems of internal accounting controls.

SEC Jurisdiction and Findings

The SEC launched the current investigation to determine whether any of nine corporate victims of cyber fraud violated Section 13(b)(2)(B)(i) and (iii) of the Securities Exchange Act of 1934, which required each of them to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that "transactions are executed" and "access to assets is permitted" only in accordance with management's general or specific authorization.

The nine public issuers suffered a combined loss of nearly $100 million as victims of a broader, pervasive cyber-related fraud scheme that has existed at least since 2013 with total losses exceeding $5 billion. Each of the nine companies lost at least $1 million, and two of them lost more than $30 million. The companies in question came from multiple industry sectors, including financial, technology, and energy, as well as machinery, real estate, and consumer goods.

The fraud campaigns took one of two forms: (i) spoofed emails claiming to be from corporate executives that typically requested midlevel finance personnel to wire money to foreign bank accounts as further instructed by spoofed outside counsel emails; and/or, (ii) real emails coming from hacked email accounts of real vendors in which the hackers requested victims to pay invoices using revised bank account information. According to the SEC, the spoofed executive scams often contained spelling and grammatical errors, while the fake vendor emails

1 SEC Release No. 84429, dated October 16, 2018 (available here).

appeared more legitimate. Regardless, the SEC concluded that neither of the frauds were sophisticated, but merely used technology "to search for both weaknesses in policies and procedures and human vulnerabilities that rendered the control environment ineffective."[2] Many of the frauds succeeded because company personnel did not follow the company's existing controls, while others succeeded because employees did not recognize the indicia of fraud contained in the emails. In many instances company employees asked no questions about the fraudulent requests, even when those requests fell "clearly outside of the employee's domain."[3]

By emphasizing that the frauds were not sophisticated in design, the SEC implied that, had the companies implemented and followed reasonable controls, they would not have fallen victim. Indeed, the Commission noted that each company took steps after the fact to improve its payment authorization procedures and verification requirements for vendor payment instruction changes. The companies also improved their training programs to enable employees to recognize relevant threats and better understand company policies and procedures designed to prevent fraud.

Nonetheless, despite the fact that the threat was widespread, well-known, had existed for years, and could have been stopped using readily available and inexpensive controls, the SEC declined to take enforcement action in any of these nine instances. Instead, the Commission expressed forward looking expectations for public companies to pay particular attention to devising and maintaining internal accounting controls designed to ensure that funds are transferred only with management's approval and/or only according to guidelines set forth by management. The SEC warned that, "issuers should be mindful of the risks that cyber-related frauds pose and consider, as appropriate, whether their internal accounting control systems are sufficient to provide reasonable assurances in safeguarding their assets from these risks."[4]

Practical Considerations

The SEC expects issuers to have effective internal accounting controls, and to review and update them based on the ever-changing risk environment. By stating that the issuers "are in the best position to develop internal accounting controls that account for their particular operations needs and risks in complying with Section 13(b)(2)(B)," the SEC appears consistent in its messaging that it will not second guess good faith judgements about how public companies are developing their internal accounting controls. The SEC's investigation of cyber-related fraud also is consistent with the interpretive guidance the Commission issued earlier in 2018 regarding the materiality of cybersecurity risk to a company's public disclosures, in which it warned companies that falling victim to successful cyber-attacks or other cybersecurity incidents may result in substantial financial costs. The Commission followed that guidance with a succession of actions, including a $35 million fine against Yahoo for failing to timely disclose a data breach and a $1 million settlement with Voya Financial Advisors after a customer data breach.

Although no enforcement actions were brought against the companies described in the Report, the SEC is sending a clear signal that it is prepared to potentially bring similar actions in the future. Issuers that do not implement, maintain and regularly update internal accounting controls that reasonably safeguard against cyber-related frauds, and train employees appropriately about threats, are at risk not only of damaging cyber breaches but also of costly violations of the federal securities laws. Put in context, the SEC's cyber-related fraud investigation serves as an additional reminder to publicly traded companies and their Boards that cybersecurity risk must be understood and overseen at the enterprise level, and a failure to do so increasingly is likely to result in material deficiencies in compliance, harm to the bottom line, and the risk of regulatory consequences.

2 Id. at 5.

3 Id. at 6.

4 Id. at 7.

White & Case LLP
701 Thirteenth Street, NW
Washington, District of Columbia 20005-3807
United States

T +1 202 626 3600