SEC Warns Companies of Potential Internal Accounting Control Violations with Business Email Compromise

October 18, 2018

Key Points

- The SEC issued guidance in the form of a rare "21(a) report" this week after investigating a series of email frauds impacting 9 unnamed companies.
- These email-based frauds, referred to as "CEO scams" or "vendor scams," were technologically unsophisticated attacks involving millions of dollars of unauthorized or misdirected wire transfers.
- Although the SEC declined to penalize the potentially offending companies, this Report signals the SEC's continued interest in the cybersecurity area, and companies are well-advised to review and bolster policies currently in place to guard against these sorts of attacks.

Following the SEC's announcement of its first Identity Theft Red Flags Rule enforcement action stemming from a cybersecurity breach, the SEC has published a Section 21(a) Report detailing an investigation into public companies that were victims of cyber-related frauds perpetrated via email. In the report, the SEC identifies a particular subset of email fraud, in which perpetrators pose either as executives or current vendors, as a significant and alarming trend, costing companies $5 billion since 2013, with an estimated $675 million lost by companies in 2017 alone. These email spoofs—sometimes called "CEO scams," "vendor scams," or "business email compromise"—do not require technologically sophisticated hacks, but instead exploit common policies and procedures concerning wire transfers and other payments. Perpetrators often target corporate finance departments in an effort to reroute planned wire payments or generate new transfers to offshore accounts. This brand of scam reportedly caused the highest estimated out-of-pocket losses from any class of cyber-facilitated crime in the same period.

This report may be interpreted as a shot across the bow for SEC Reporting Companies, indicating that the SEC intends to further heighten scrutiny in the cybersecurity space, and pursue enforcement actions against public companies that fail to take reasonable measures to safeguard against email spoofing attacks.

Contact

Natasha G. Kohne
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
mreed@akingump.com
Dallas
+1 214.969.2713

Peter I. Altman
paltman@akingump.com
Los Angeles
+1 310.728.3085

Nicholas C. Adams
nadams@akingump.com
San Francisco
+ 1 415.765.9529

Lauren E. York
lyork@akingump.com
Dallas
+1 214.969.4395

What is a 21(a) Report?

A 21(a) report is an investigative report that allows the SEC to communicate to the public about certain problematic areas or sets of concerns without penalizing potentially offending companies.

These reports are fairly rare; this is the first of 2018, and there was only one in 2017 (covering whether certain blockchain assets could be classed as securities). Because of the relative scarcity of 21(a) reports, businesses are wellserved to pay attention to the guidance of the SEC contained in the reports.

Summary of the Report

The SEC investigated these victim companies for violations of Section 13(b)(2)(B) of the Securities Exchange Act of 1934, which requires SEC Reporting Companies (i.e., those with an obligation to report under Section 12 of the Securities Exchange Act) to devise and maintain internal accounting controls to provide reasonable assurances that transactions are executed with management's authorization. In essence, Section 13(b)(2)(B) aims to hold Reporting Companies responsible as stewards of the public's dollars by ensuring that company employees take appropriate steps to prevent payment fraud and embezzlement. The SEC investigated whether nine unnamed public companies that these scams targeted may have run afoul of the federal securities laws by failing to have sufficient systems of internal accounting controls to detect that the incoming wire requests were fraudulent. Ultimately, the SEC determined that the victim issuers' conduct fell short of warranting an enforcement action, but the investing public and other issuers would be well-served by learning from their experience.

While the perpetrators described in the report apparently brought different levels of sophistication to their efforts, at the bottom the scams themselves were not complex. In the so-called "CEO scam," perpetrators created similar-looking email address to the CEO of a company from which they could send emails requesting wire transfers to foreign banks. In each of the instances detailed in the report, the spoofed emails stressed that the receiving employee should keep the request secret from others at the company, because it was a confidential "deal" that merited secrecy and confidentiality, at times even raising the specter of scrutiny from the SEC to induce employees to not question the unusual requests. The second scam involved perpetrators who impersonated the business' existing vendors by taking control of the vendor's email systems. Once inside, the perpetrators inserted illegitimate requests for payments into otherwise legitimate invoices, and/or asked for the business' employees to change banking information to direct payments to fraudulent accounts.

Practical Steps & Key Takeaways

This report does not detail specific cybersecurity requirements for companies, but the examples provided suggest concrete steps that companies should take to protect themselves against this type of fraud (e.g., enhanced employee training on policies and procedures, two-factor confirmation of wire transfers, bolstering account verification procedures to aid in detection, and so forth).

Based on our experience advising companies on how to best protect from cyberattacks, we recommend that company management be prepared to defend and explain their procedures and policies to protect companies (and their shareholders) from such wire fraud:

- Ensure that there are policies in place covering proper procedure for initiating or changing wire transfers.
  - These policies should be clear, widely distributed and enforced. They should also be tailored to particular industry-specific risks or processes.
- Implement strong safeguards that help correct for human error.
  - At a minimum, two-level authentication involving high-level employees should be used for significant wire transfers.
  - Consider requiring multiple confirmation mediums, such as through email, phone, and if possible, in-person communication.
  - Bolster account reconciliation procedures and outgoing payment notification processes to aid in detection of payments.
- Train employees at all levels consistently and enforce the policies and procedures.
  - Employees should be trained on spotting red flags for these scams, including misspellings in the emails, requests that they acquire wire details from an outside consultant, insistence on secrecy, rushed requests, wires to unusual banking institutions and nonstandard email addresses.
  - Employees should also be trained that certain requests should always receive heightened scrutiny, including requests while the CEO or other executives are traveling or unavailable, or requests that the account number or bank be switched in the midst of the transaction.
  - Employees should initiate their own chain of confirmation by separately e-mailing executives, vendors and bank personnel at known addresses, calling them at their ordinary phone numbers or visiting them in-person. This can help thwart more sophisticated spoofers who seek to defeat multifactor authentication by instructing the target to call a new phone number for confirmation.
- Review insurance coverage to ensure these types of scams are covered
  - Having a comprehensive errors and omissions policy along with a cybersecurity policy will ensure that coverage in the event of a wire fraud is not denied due to the level of computer and network involvement, or an error on the part of an employee. New policies are also being written specifically with these types of scams in mind.