Updates
October 24, 2018

SEC 21(a) Report Warns Public Company Email Scam Victims of Bigger Problems Than Stolen Money

Known by many names, including business email compromise fraud, CEO or CFO fraud, impersonation attacks, or "Man-in-the-Email" scams, cyber-related frauds involving spoofed or otherwise compromised business electronic communications continue to be an increasingly pervasive threat to businesses of all sizes, including public companies. As the FBI announced in July 2018, business email compromise/email account compromise fraud has affected victims in all 50 states and 150 countries, resulting in actual and attempted losses of over $12 billion since 2013.

In response to the threat posed by business email compromise and other cyber-related frauds to public companies, on October 16, 2018 the U.S. Securities and Exchange Commission (SEC) issued an investigative report under Section 21(a) of the Securities Exchange Act of 1934 (1) describing its findings following the investigation of nine public company victims, and (2) warning public companies that internal mistakes and lapses that enable successful business email compromise and other cyber-related frauds may indicate failures by the companies to maintain sufficient internal accounting controls, as required under Section 13(b)(2)(B) of the Exchange Act.

Background: The Threat and Past SEC Guidance

A business email compromise is a phishing scheme that frequently involves a cybercriminal impersonating a company executive or vendor in an attempt to lure employees to transfer funds or release sensitive personal information, including personally identifiable information. Unlike most mass-phishing schemes, business email compromises are highly targeted attacks. Cybercriminals will scour hacked email accounts, research employees on social media outlets and other websites, follow company news and learn about specific goods coming from specific vendors to convincingly impersonate executives and vendors.

And, these schemes are working. The FBI reports that business email compromises have caused the highest estimated out-of-pocket losses of any class of cyber-facilitated crime committed during the last five years. Asian banks in China and Hong Kong are the primary destinations for fraudulent fund transfers, but banks in the United Kingdom, Mexico and Turkey also have been identified as transfer targets.

In February of 2018, the SEC issued a formal interpretative release on public company disclosure obligations regarding cybersecurity. The February guidance emphasized that "cybersecurity presents ongoing risks and threats to our capital markets and to companies operating in all industries, including public companies" and advised that "[c]ybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with federal securities laws." The Section 21(a) Report marks the latest in SEC guidance regarding cybersecurity risks.

Recent Section 21(a) Report

The SEC's Division of Enforcement (Enforcement), in consultation with the Division of Corporation Finance and the Office of the Chief Accountant, launched an investigation into nine public companies that fell victim to business email compromises, asking whether the companies may have violated the federal securities laws by failing to have a sufficient system of internal accounting controls. In its Section 21(a) Report, dated October 16,

2018, the SEC announced that it would not pursue enforcement actions in these matters. However, the SEC "deem[ed] it appropriate and in the public interest," to issue a Section 21(a) Report to make issuers aware that these threats exist and should be considered when evaluating internal accounting controls as required by the federal securities laws.

Investigation Findings

The nine companies involved in Enforcement's investigation operated in a wide range of sectors, including technology, machinery, real estate, energy, financial and consumer goods, a fact indicating vulnerabilities across all industries. In addition, each company had "substantial" annual revenues and was listed on a national securities exchange at the time of the fraud to which they fell victim.

Every company lost at least $1 million as a result of the business email compromise fraud; two lost more than $30 million. The nine companies lost nearly $100 million in total, almost all of which was not recovered. The scams were not one-time hits. One company made 14 wire payments requested by a fraudster posing as a company executive over the course of several weeks before the fraud was detected by a foreign bank alert. Another company paid eight invoices totaling $1.5 million over several months in response to a vendor's doctored paperwork for a banking change.

In reviewing email correspondence between company personnel and the perpetrators, Enforcement identified two types of business email compromise schemes:

- **CEO Impersonation.** Cybercriminals emailed company finance personnel, often mid-level employees, using spoofed email domains and addresses of a company executive. In all CEO impersonation cases, the spoofed email directed employees to work with a purported outside attorney, who then directed employees to initiate large wire transfers to foreign bank accounts controlled by perpetrators. They used real law firm and attorney names but connected employees to impersonator-lawyers.

- **Vendor Impersonation.** Perpetrators hacked into existing vendors' email accounts and inserted illegitimate requests for payments (and payment processing details) into electronic communications. They corresponded with unwitting employees responsible for procuring goods from the vendors, so they could get information about actual purchase orders and invoices, and then attached doctored invoices to correspondence with finance personnel.

Report Takeaways

Though the SEC is declining to pursue enforcement actions against these nine victim-companies, it notes that the frauds succeeded, at least in part, because of deficient payment authorization procedures, deficient verification requirements for vendor information changes, the responsible personnel's insufficient understanding of the company's existing controls and the responsible personnel's failure to recognize suspicious email correspondence.

To that end, the Report advises public companies to "pay particular attention to the obligations imposed by Section 13(b)(2)(B) to devise and maintain internal accounting controls that reasonably safeguard" company and investor assets from cyber-related frauds. The Report specifically points to Section 13(b)(2)(B)(i) and (iii), which require certain 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 that "(iii) access to assets is permitted only in accordance with management's general or specific authorization." The Report concludes by encouraging companies to be mindful of the risks and to consider, as appropriate, whether their internal accounting control systems are sufficient to provide reasonable assurances.

The SEC's decision to not pursue actions against the nine investigated companies and the "advisory" tone taken in the Report's language, should not be interpreted as an indication that future public company-victims of business email compromise or other cyber-related frauds will escape Enforcement scrutiny. As demonstrated by the enforcement actions against unregistered cryptocurrency offerings following issuance of the SEC's related Section 21(a) Report, the agency is willing to punctuate its public guidance with litigation against those who do not heed its warnings.

Practical Tips

Based on the Report highlights described above, particularly the SEC's advice to reassess existing internal accounting controls, we offer the following practical tips to public companies:

1. **Dual-Factor Authentication.** For a business email compromise scheme to be successful, scammers must first phish executives or vendors to gain access to their email accounts. Dual-factor authentication, which grants access to the user only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism, makes it much more difficult for perpetrators to gain access to vulnerable personnel email inboxes.
2. **Verification Requirements for Bank/Vendor Information Changes.** Business email compromise scammers often request that payments originally scheduled for check dispersal be sent via wire instead. Verification requirements will help ensure that all requests for a change in payment type and/or location are legitimate.
3. **Training—Teach Employees What to Look For.** In its Report, the SEC identified several "common elements" associated with "fake executive" emails, including time-sensitive "deals" with the need for secrecy, requested funds needed for foreign transactions, mid-level personnel as targets and grammatical errors in the correspondence. Scheme detection is more likely when employees are educated about red flags and warning signs.

For more information and practical tips for responding to business email compromise and other cyber-related frauds, please see Perkins Coie's June 2015 update entitled "Worldwide CEO-CFO Cyber Scam: Prevention and Recovery Tips."

Remember, time is of the essence once a fraud has been discovered. Prompt notification to experienced counsel, financial institutions and, if appropriate, law enforcement agencies and insurance providers can be critical to the effectiveness of recovery attempts.

Authors

Allison C. Handy

Partner
AHandy@perkinscoie.com 206.359.3295

Explore more in

Corporate Governance | Public Companies | White Collar & Investigations | Securities Litigation | Privacy & Security | Corporate Law

Related insights

Update

Ninth Circuit Rejects Mass-Arbitration Rules, Backs California Class Actions

Update

CFPB Finalizes Proposed Open Banking Rule on Personal Financial Data Rights