Morgan Lewis

LAWFLASH

SEC ISSUES REPORT ON CYBER FRAUD AGAINST PUBLIC COMPANIES, INTERNAL CONTROL REQUIREMENTS

October 31, 2018

AUTHORS AND CONTACTS

Susan D. Resley, Mark L. Krotoski, Jillian Harris

The US Securities and Exchange Commission's Division of Enforcement (SEC) issued an investigative report on October 16 on nine public companies that were victims of cyber-related frauds, and considered whether these companies violated federal securities laws by failing to have a sufficient system of internal accounting controls. While the SEC did not pursue any enforcement action based on its findings, the report highlights the pervasiveness of cyber-related fraud and states that public companies could still be liable for federal securities violations if they do not have sufficient internal accounting controls that specifically take into account these new threats. This report builds upon the SEC's previous cybersecurity disclosure guidance, which the agency voted unanimously to approve.[1]

The report, issued pursuant to Section 21(a) of the Exchange Act,[2] outlines the scope of the SEC's investigation: specifically focusing on two variants of cyber-fraud schemes involving "business email compromises" (BECs). The FBI defines BEC as a "sophisticated scam targeting businesses that often work with foreign suppliers and/or businesses and regularly perform wire transfer payments."[3] The companies investigated cover a range of sectors, each having substantial annual revenues and securities listed on a national securities exchange, reflecting the "reality that every type of business is a potential target of cyber-related fraud."[4] This report reflects the SEC's increased attention on the enforcement of cybersecurity issues.[5] On September 25, 2017, the SEC announced the establishment of a "Cyber Unit" designed to "focus the Enforcement Division's substantial cyber-related expertise on targeting cyber-related misconduct."[6]

BROAD IMPACT AND VARIATIONS OF BEC SCHEMES

BEC schemes have hit numerous companies and can cost its victims tens of millions of dollars, and sometimes, a large portion of a company's capital.[7] The BEC schemes can take many forms. These fraud schemes typically involve a form of social engineering to persuade others to transfer funds or data to a new account. Based on the manner of the communication, the victim believes the request is legitimate when it is

not.

Common schemes include cyber thieves taking over a business email account and sending fraudulent invoices to company customers, then requesting payment at a new bank account, typically outside the United States, or asking company subordinates to send a wire to a particular bank account. Because the request comes from a known business account, it appears to be legitimate. Another variation involves a modified email account, such as obtaining a domain for compenyA.com instead of companyA.com. The recipients may not notice the new domain. The cyber thieves control the communications at a new domain and direct the transfer of funds to a bank account they control. The BEC scheme has also been used to request confidential or sensitive data – instead of fraudulent wire transfers. The cyber thieves try to monetize the data, such as redirected taxpayer identification numbers, social security numbers, or proprietary information.[8]

The FBI estimates that BECs have caused over $5 billion in losses since 2013, with an additional $675 million in adjusted losses in 2017 – the highest estimated out-of-pocket losses from any class of cyber-facilitated crime during this period.[9] Federal officials have arrested and prosecuted individuals involved in the BEC schemes.[10]

SEC INVESTIGATION REPORT FOCUS

The report underscored the severity of cyber-related frauds, stating that each of the nine companies lost at least $1 million; two lost more than $30 million, and in total, the nine public companies lost nearly $100 million, almost none of which was recovered.

One BEC scheme involved a scammer purporting to be a high-level executive emailing a directive to employees in the company's finance group to work with an outside law firm or attorney to wire large sums of money to a foreign bank. The scammer generally spoofs the email domain and address of the executive to make the correspondence look legitimate. These schemes generally shared the same characteristics: (1) time sensitivity and secrecy; (2) use of funds for foreign transactions or acquisitions; (3) targeted to mid-level employees who would not otherwise be in charge of such a transaction. While these "were not sophisticated frauds in general design or the use of technology,"[11] these schemes were only uncovered when they were flagged by other foreign banks and law enforcement.

The second BEC ploy involved a scammer purporting to be an existing vendor.[12] These more sophisticated schemes involved the hacking of email accounts of the victim companies' foreign vendors. The scammers then made illegitimate requests for payment and communicated with the company personnel responsible for procuring goods in order to gain access to information about actual purchase orders and invoices. As a result, the personnel made illegitimate payments to the foreign accounts of the scammers instead of the real vendors. Because these scams had fewer red flags, several victims learned of the scams only when their vendors raised concerns about unpaid invoices.

NEED FOR INTERNAL CONTROLS

Based on these findings, the SEC advised that public companies should actively devise and maintain internal accounting controls that reasonably safeguard company and investor assets from cyber-related frauds. Specifically, the report highlighted the obligations under Section 13(b)(2)(B)(i) and (iii) of the

Securities Exchange Act, which requires public companies 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."[13] As noted above, some of the BEC fraud schemes were not particularly sophisticated but instead, "relied on technology to search for both weaknesses in policies and procedure and human vulnerabilities that rendered the control environment ineffective."[14]

FURTHER GUIDANCE AND A WARNING TO VICTIMS

The SEC has made no secret of its efforts to stop hackers who "[reap] more than $100 million in illicit profits by stealing nonpublic information and trading based on that information."[15] It has also brought actions against registered entities that were the victims of a hacking scheme, in part because of the highly sensitive information held by financial institutions and other regulated firms. For example, in one settled action, the SEC found that a registered investment adviser completely failed to establish reasonable cybersecurity policies and procedures to protect customer records and information, after an unknown hacker gained access to the server, and compromised the personally identifiable information of approximately 100,000 individuals. In so doing, the SEC's order noted, "Taken as a whole, R.T. Jones's policies and procedures for protecting customer records and information were *not reasonable to safeguard customer information*."[16] Finally, the SEC has brought actions against an issuer under the anti-fraud provisions for failing to disclose a significant breach.[17]

The recent 21(a) report, however, is the first time that the SEC signaled its willingness to pursue enforcement actions *against public company victims* of cyber-related crimes for failure to have sufficient internal controls to prevent the cyber-crime. While the report does take the time to note that not every victim is also in violation of the federal securities laws, "[w]hat is clear, however, is that internal accounting controls may need to be reassessed in light of emerging risks [. . .] Public issuers subject to the requirements of Section 13(b)(2)(B) *must* calibrate their internal account controls to the current risk environment and assess and adjust policies and procedures accordingly."[18]

Its statement concerning the need to "calibrate" controls is key: simply implementing any system of internal controls will be insufficient.[19] As with any system of internal controls, that control must be customized and executable. Not surprisingly, the SEC pointed to a company's need to provide training to employees on how to spot schemes, highlighting numerous examples of where the frauds succeeded because the responsible personnel did not sufficiently understand the company's existing controls or did not recognize the emails lacked reliability.

IS YOUR COMPANY READY FOR A BEC EVENT?

With this report, the SEC has signaled that it will not only pursue "the bad guys," but will scrutinize a company's controls designed to detect and prevent hacking schemes. This represents a significant development in the obligations and expectations of public companies' internal accounting controls. More than ever, a company must ask whether they—and more importantly, their employees—are prepared to recognize and prevent a catastrophic BEC event that could compromise the fraudulent transfer of funds or sensitive data.

Morgan Lewis has assisted numerous companies that were targeted by BEC schemes and has helped them in designing appropriate controls. Depending on the circumstances, some of the following steps in assessing their internal controls systems may be considered:

- **Conflrmation of Transaction**: Implementing a non-email verification process (such as separate telephone confirmation) for transactions over a threshold amount (e.g., telephoning a superior to confirm they initiated the request)
- **Separate Authorization**: Mandating that the employee initiating a wire transfer must have separate authorization before sending the wire transfer
- **Designated Contacts**: Designate an authorized contact person for each financial account, who is the only person at the vendor and/or company who has the authority to request payment or changes to an existing contract or invoice
- **Policies**: Reviewing and updating policies such as requiring authorization to change bank deposit information and contact information
- **Limiting Access**: Closely manage access to privilege identity and access management (PAM)
- **Financial Institution Protocols**: Implement controls with financial institutions, specifically designating a specific person and a telephone authorization for certain transactions or transactions over a threshold amount
- **Training**: Actively training personnel on relevant policies, as well as how to recognize spoofed emails or other attributes of BEC, and to be alert to phishing schemes
- **Detection and Blocking**: Work with the chief information security officer (CISO) and IT department to detect unauthorized access to company email accounts. For example, monitor email exchange servers to check changes in configuration and custom rules on key accounts
- **Incident Response**: Include BEC schemes as part of your incident response plan and table-top testing. Consider including financial institution contact information to be able to take steps to stop the fraudulent transfer and recover funds. The ability to detect the fraudulent transfer as quickly as possible may enhance the possibility of recovering the funds
- **Legal Review**: Ensure your policies and controls are reviewed to prevent and detect cybercrime given the heightened focus by the SEC and other federal and state agencies on whether the company as a victim has appropriate policies and procedures in place

CONTACTS

If you have any questions or would like more information on the issues discussed in this LawFlash, please contact any of the following Morgan Lewis lawyers:

Boston
Timothy P. Burke

Chicago
Peter K.M. Chan

London
Pulina Whitaker

New York
Ben A. Indek
Mary Gail Gearns

Philadelphia
Gregory T. Parks

San Francisco
W. Reece Hirsch
Susan D. Resley

Silicon Valley
Mark L. Krotoski

Washington, DC
Amy J. Greer
Ivan P. Harris

---

[1] *See* LawFlash, *SEC Issues Guidance on Cybersecurity Disclosures* (Feb. 28, 2018).

[2] 15 U.S.C.A. § 78u (a).

[3] Federal Bureau of Investigation, 2017 Internet Crime Report at 12 (May 7, 2018) (hereafter FBI Internet Crime Report).

[4] Securities and Exchange Commission, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements, Release No. 84429 (October 16, 2018) (hereinafter Report).

[5] The SEC has brought enforcement actions including in April and September. *See* Securities and Exchange Commission Press Release, *SEC Charges Firm With Deficient Cybersecurity Procedures* (Sept. 26, 2018); Securities and Exchange Commission Press Release, *Company Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million* (April 24, 2018).

[6] *See* Securities and Exchange Commission Press Release, *SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors* (September 25, 2017).

[7] Kate Fazzini, *CFTC Settlement Shows New Era of Third Party Cyberrisk*, The Wall Street Journal (October 4, 2017) (detailing how commodity pool operator Tillage Commodities Management LLC lost $5.9 million, 64% of its total capital, in BEC scheme and was subsequently fined by the CFTC); Robert Hackett, *Fraudsters Duped this Company into Handing over $40 million*, Fortune (August 10, 2015) (detailing how networking equipment company Ubiquiti Networks lost $46.7 million dollars in a BEC scam).

[8] Internet Crime Complaint Center, Business E-Mail Compromise, E-Mail Account Compromise, The 5 Billion Dollar Scam (May 4, 2017) (Alert Number I-050417-PSA) (describing "five main scenarios").

[9] *See* FBI Internet Crime Report, at 4, 21.

[10] US Dep't of Justice Press Release, *74 Arrested in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes* (June 11, 2018).

[11] Report, at 3.

[12] Although the SEC's report focused on only two types of schemes, the FBI Internet Crime Report outlined another scheme perpetuated in 2016, which involved the compromise of legitimate business email accounts and fraudulent requests for personally identifiable information or W-2 states for employees. *See* FBI Internal Crime Report, at 12. The report also outlined several other types of cybercrimes, including confidence fraud, personal data breach, identity theft, credit card fraud, etc. *Id.* at 21.

[13] 15 U.S.C.A. § 78m(b)(2)(B)(i) and (iii).

[14] Report, at 5.

[15] Securities and Exchange Commission Press Release, *SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases* (August 11, 2015).

[16] Securities and Exchange Commission, Order Instituting Administrative and Cease-And-Desist Proceeding Pursuant To Sections 203(e) and 203(k) of the Investment Advisers Act of 1940, Making Findings, and Imposing Remedial Sanction and a Cease-and-Desist Order, Release No. 4204, at 3 (September 22, 2015).; *see also* Securities and Exchange Commission Press Release, *SEC: Morgan Stanley Failed to Safeguard Customer Data* (June 8, 2016).

[17] *See* Securities and Exchange Commission Press Release, *Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million*, (April 24, 2018).

[18] Report, at 6.

[19] *Id.* at 5-6.