Client Alert: SEC Warns Corporations about BEC Attacks

On Oct. 16, 2018, the SEC issued a type of report, known as a "21(a) Report," on Business Email Compromise ("BEC") attacks.[i] The report warrants careful examination as these 21(a) reports often function as a warning to public companies and their counsel that enforcement charges could be brought in similar circumstances in the future. Thus, a successful BEC attack may, in certain circumstances, now raise the risk of an SEC investigation and enforcement action.

What is a Business Compromise Email Attack?

BEC attacks come in many forms. But they often resemble one of the following two scenarios.

SCENARIO 1

Attackers begin by impersonating a company executive using spoofed email domains and addresses in an attempt to appear legitimate.

Attackers will then use the fake email account to prompt an employee (usually in the finance department) to make a wire deposit to a particular account number under the guise of an innocuous transaction.

Note that BEC attacks of this type do not require a sophisticated hacker's skillset. No infiltration of firewalls or the company's physical security is needed, though such an intrusion could make the fraud even more difficult to detect (because the executive's email might then come from the executive's actual email account). The attacker simply needs to register a domain name that appears similar to the victim company's real domain name and then can use web searches, online biographies, and social network sites to identify the names of relevant executives and finance department employees.

SCENARIO 2

Attackers begin by hacking a vendor's actual email account.

Attackers obtain actual purchase orders and invoices from the target company's personnel.

Attackers generate fake invoices directing payment to a new attacker-controlled account.

These vendor-based attacks are particularly challenging for victims to detect because they use a vendor's legitimate email account and the manipulation of legitimate invoices. Also, because vendors may wait months before asking about missing invoices (which the company believed it had already paid), it is possible for these attacks to occur over a substantial period of time.

Recognizing BEC Attacks

Although BEC attacks are by their very nature intended to deceive, the SEC's 21(a) Report identifies certain red flags that are typically seen in these attacks:

- Describing time-sensitive transactions and/or conveying a sense of urgency for the wire.
- Lack of significant details about the supposed deal.
- Conveying the need for secrecy from other company employees.
- Suggesting that the transaction is occurring with government oversight.
- Spelling and grammatical errors.
- Directing a member of the finance staff to work with outside attorneys to effectuate the wire transfers to a foreign bank or recipient.

Note that while the existence of one, or some combination, of the above red flags may not conclusively indicate the presence of a BEC attack, the more red flags that are present in a suspicious email, the more likely an email is a BEC attack. As attackers become more sophisticated, so too will their deception techniques. Ongoing training and education therefore are important.

The SEC's Role in Public Company Cybersecurity

The SEC's BEC report is focused on "internal accounting controls" pursuant to Section 13(b)(2)(B) of the Securities Exchange Act. That provision requires issuers to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that transactions are executed with, or that access to company assets is permitted only with, management's general or specific instructions.

The BEC report was prompted by the Enforcement Division's investigation of nine publicly traded companies that were victims of BEC attacks. All nine lost millions of dollars through BEC attacks. The SEC did not bring charges against the victims, but it used the occasion "to make issuers and other market participants aware that these cyber-related threats of spoofed or manipulated electronic communications exist and should be considered when devising and maintaining a system of internal accounting controls as required by the federal securities laws."[ii]

The BEC report signals that the SEC might take action against issuers whose internal controls are insufficient even where the vulnerability does not render the issuers' financial reports misleading. And issuers should expect their auditors to make inquiries informed by the BEC report when they consider the issuers' internal controls.

Potential Enhancements to Accounting Controls

The report states that the SEC "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 of the federal securities laws." But it cautions "that internal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds. Public issuers subject to the requirements of Section 13(b)(2)(B) must calibrate their internal accounting controls to the current risk environment and assess and adjust policies and procedures accordingly."[iii]

The BEC report suggests several ways in which public issuers can enhance their accounting controls, reduce the risk of a successful BEC attack, and mitigate the chance of an SEC enforcement action or investigation. Companies should:

- Companies should ensure they have robust cybersecurity training programs in place for their employees. In addition to phishing and password protection, a company's cyber education should include training on how to prevent BEC attacks. In particular, accounting employees should be trained on identifying potential signals of a BEC attack.
- Effective training should address policies and procedures related to payments to third parties. Strong accounting control programs should include education practices designed to teach and remind employees of important approval and verification processes.
- Companies should assess whether their current approval and verification procedures are adequate. It may be reasonable to examine whether executive approval for significant payments should be conveyed orally or through some other reliable channel (and not merely through a high-level executive's email requesting the payment), or require the use of code words. A company may also want to require that its employees obtain verbal confirmation from venders of any change to its account payment instructions by calling a phone number that the employee independently knows is associated with the account. The best solution will vary based on a company's circumstances.
- Companies should evaluate whether their systems for detecting BEC fraud are adequate. For example, a company may want to institute a process where significant payments to foreign recipients trigger additional review by someone knowledgeable about BEC attacks and who was uninvolved in the initial payment. Where a BEC attack does succeed, a company should reassess the adequacy of its accounting controls.
- Companies should consider whether there are other current or emerging cyber threats that could also implicate their duty to maintain sufficient internal accounting controls.

---

[i] Securities and Exchange Commission, Release No. 84429, 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 (Oct. 16, 2018) (hereinafter "Section 21(a) Report").

[ii] Section 21(a) Report at 2.

[iii] Section 21(a) Report at 6.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Munger, Tolles & Olson lawyer with whom you normally consult:

George M. Garvey
Partner
(213) 683-9153
George.Garvey@mto.com

Grant A. Davis-Denny
Partner
(213) 683-9225
Grant.Davis-Denny@mto.com

Nefi D. Acosta
Associate
(213) 683-9564
Nefi.Acosta@mto.com

Najee K. Thornton
Associate
(213) 683-9284
Najee.Thornton@mto.com