The Debrief

SEC Investigation Report: Internal Accounting Controls Must be Calibrated to Cyber Risk

October 17, 2018

On October 16, 2018, the SEC issued a Report of Investigation (the "Report") to underscore the threat of spoofed or manipulated electronic communications and to urge reporting companies to calibrate internal accounting controls to the current risk environment and assess and adjust internal policies and procedures accordingly.

Debevoise & Plimpton

The SEC investigated nine listed companies in a range of industries that were victims of fraud (emails from fake executives or fake vendors) to determine whether the companies violated federal securities laws by failing to maintain adequate internal accounting controls. Each company lost at least $1 million; two lost more than $30 million.

Federal securities laws require that public companies maintain internal accounting controls sufficient to provide reasonable assurances that transactions are executed with, and that access to company assets is permitted only with, management's general or specific authorization. The Report notes that while the victimized companies had procedures in place that required certain levels of authorization for payment requests, outgoing wires and verification of changes in vendor data, the ultimately compromised emails were designed to search for both weaknesses in policies and procedures and human vulnerabilities that rendered the existing control environment ineffective.

To that end, the Report highlighted certain efforts by these companies to enhance their internal accounting controls after falling victim to fraud, including:

- Improving payment authorization procedures and verification requirements for vendor information changes
- Bolstering account reconciliation procedures and outgoing payment notification processes
- Enhancing training of responsible personnel about relevant threats as well as about pertinent policies and procedures

While the SEC determined not to take enforcement action against the victimized companies, it emphasized that having internal accounting controls that factor in cyber-related threats and related human vulnerabilities may be vital to maintaining a sufficient accounting control environment. We note that an arguably similar fake vendor scam perpetrated on Voya Financial Advisors resulted in a recent SEC enforcement order based on the customer record and information safeguards applicable to broker-dealers and investment advisers registered with the SEC.

The Report serves as a good reminder to SEC reporting companies to review their policies and procedures against the current cyber-threat environment and internal accounting control requirements. The Report should be read together with the SEC's February 2018 Guidance regarding cybersecurity disclosure and governance requirements applicable to SEC reporting companies.

Luke Dembosky
Partner, Washington, D.C.
+ 1 202 383 8020
ldembosky@debevoise.com

Jeremy Feigelson
Partner, New York
+ 1 212 909 6230
jfeigelson@debevoise.com

Matthew E. Kaplan
Partner, New York
+ 1 212 909 7334
mekaplan@debevoise.com

Jim Pastore
Partner, New York
+1 212 909 6793
jjpastore@debevoise.com

Paul M. Rodel
Partner, New York
+1 212 909 6478
pmrodel@debevoise.com

Steven J. Slutzky
Partner, New York
+1 212 909 6036
sjslutzky@debevoise.com

Joel D. Salomon
Associate, New York
+ 1 212 909 6458
jsalomon@debevoise.com