GIBSON DUNN

October 17, 2018

SEC WARNS PUBLIC COMPANIES ON CYBER-FRAUD CONTROLS

To Our Clients and Friends:

On October 16, 2018, the Securities and Exchange Commission issued a report warning public companies about the importance of internal controls to prevent cyber fraud. The report described the SEC Division of Enforcement's investigation of multiple public companies which had collectively lost nearly $100 million in a range of cyber-scams typically involving phony emails requesting payments to vendors or corporate executives.[1]

Although these types of cyber-crimes are common, the Enforcement Division notably investigated whether the failure of the companies' internal accounting controls to prevent unauthorized payments violated the federal securities laws. The SEC ultimately declined to pursue enforcement actions, but nonetheless issued a report cautioning public companies about the importance of devising and maintaining a system of internal accounting controls sufficient to protect company assets.

While the SEC has previously addressed the need for public companies to promptly disclose cybersecurity incidents, the new report sees the agency wading into corporate controls designed to mitigate such risks. The report encourages companies to calibrate existing internal controls, and related personnel training, to ensure they are responsive to emerging cyber threats. The report (issued to coincide with National Cybersecurity Awareness Month) clearly intends to warn public companies that future investigations may result in enforcement action.

The Report of Investigation

Section 21(a) of the Securities Exchange Act of 1934 empowers the SEC to issue a public Report of Investigation where deemed appropriate. While SEC investigations are confidential unless and until the SEC files an enforcement action alleging that an individual or entity has violated the federal securities laws, Section 21(a) reports provide a vehicle to publicize investigative findings even where no enforcement action is pursued. Such reports are used sparingly, perhaps every few years, typically to address emerging issues where the interpretation of the federal securities laws may be uncertain. (For instance, recent Section 21(a) reports have addressed the treatment of digital tokens as securities and the use of social media to disseminate material corporate information.)

The October 16 report details the Enforcement Division's investigations into the internal accounting controls of nine issuers, across multiple industries, that were victims of cyber-scams. The Division identified two specific types of cyber-fraud – typically referred to as business email compromises or "BECs" – that had been perpetrated. The first involved emails from persons claiming to be unaffiliated corporate executives, typically sent to finance personnel directing them to wire large sums of money to

a foreign bank account for time-sensitive deals. These were often unsophisticated operations, textbook fakes that included urgent, secret requests, unusual foreign transactions, and spelling and grammatical errors. The second type of business email compromises were harder to detect. Perpetrators hacked real vendors' accounts and sent invoices and requests for payments that appeared to be for otherwise legitimate transactions. As a result, issuers made payments on outstanding invoices to foreign accounts controlled by impersonators rather than their real vendors, often learning of the scam only when the legitimate vendor inquired into delinquent bills.

According to the SEC, both types of frauds often succeeded, at least in part, because responsible personnel failed to understand their company's existing cybersecurity controls or to appropriately question the veracity of the emails. The SEC explained that the frauds themselves were not sophisticated in design or in their use of technology; rather, they relied on "weaknesses in policies and procedures and human vulnerabilities that rendered the control environment ineffective."

SEC Cyber-Fraud Guidance

Cybersecurity has been a high priority for the SEC dating back several years.

The SEC has pursued a number of enforcement actions against registered securities firms arising out of data breaches or deficient controls. For example, just last month the SEC brought a settled action against a broker-dealer/investment-adviser which suffered a cyber-intrusion that had allegedly compromised the personal information of thousands of customers. The SEC alleged that the firm had failed to comply with securities regulations governing the safeguarding of customer information, including the Identity Theft Red Flags Rule.[2]

The SEC has been less aggressive in pursuing cybersecurity-related actions against public companies. However, earlier this year, the SEC brought its first enforcement action against a public company for alleged delays in its disclosure of a large-scale data breach.[3]

But such enforcement actions put the SEC in the difficult position of weighing charges against companies which are themselves victims of a crime. The SEC has thus tried to be measured in its approach to such actions, turning to speeches and public guidance rather than a large number of enforcement actions. (Indeed, the SEC has had to make the embarrassing disclosure that its own EDGAR online filing system had been hacked and sensitive information compromised.[4])

Hence, in February 2018, the SEC issued interpretive guidance for public companies regarding the disclosure of cybersecurity risks and incidents.[5] Among other things, the guidance counseled the timely public disclosure of material data breaches, recognizing that such disclosures need not compromise the company's cybersecurity efforts. The guidance further discussed the need to maintain effective disclosure controls and procedures. However, the February guidance did not address specific controls to prevent cyber incidents in the first place.

The new Report of Investigation takes the additional step of addressing not just corporate disclosures of cyber incidents, but the procedures companies are expected to maintain in order to prevent these breaches from occurring. The SEC noted that the internal controls provisions of the federal securities laws are

not new, and based its report largely on the controls set forth in Section 13(b)(2)(B) of the Exchange Act. But the SEC emphasized that such controls must be "attuned to this kind of cyber-related fraud, as well as the critical role training plays in implementing controls that serve their purpose and protect assets in compliance with the federal securities laws." The report noted that the issuers under investigation had procedures in place to authorize and process payment requests, yet were still victimized, at least in part "because the responsible personnel did not sufficiently understand the company's existing controls or did not recognize indications in the emailed instructions that those communications lacked reliability."

The SEC concluded that public companies' "internal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds" and "must calibrate their internal accounting controls to the current risk environment."

Unfortunately, the vagueness of such guidance leaves the burden on companies to determine how best to address emerging risks. Whether a company's controls are adequate may be judged in hindsight by the Enforcement Division; not surprisingly, companies and individuals under investigation often find the staff asserting that, if the controls did not prevent the misconduct, they were by definition inadequate. Here, the SEC took a cautious approach in issuing a Section 21(a) report highlighting the risk rather than publicly identifying and penalizing the companies which had already been victimized by these scams.

However, companies and their advisors should assume that, with this warning shot across the bow, the next investigation of a similar incident may result in more serious action. Persons responsible for designing and maintaining the company's internal controls should consider whether improvements (such as enhanced trainings) are warranted; having now spoken on the issue, the Enforcement Division is likely to view corporate inaction as a factor in how it assesses the company's liability for future data breaches and cyber-frauds.

---

[1] SEC Press Release (Oct. 16, 2018), available at www.sec.gov/news/press-release/2018-236; the underlying report may be found at www.sec.gov/litigation/investreport/34-84429.pdf.

[2] SEC Press Release (Sept. 16, 2018), available at www.sec.gov/news/press-release/2018-213. This enforcement action was particularly notable as the first occasion the SEC relied upon the rules requiring financial advisory firms to maintain a robust program for preventing identify theft, thus emphasizing the significance of those rules.

[3] SEC Press Release (Apr. 24, 2018), available at www.sec.gov/news/press-release/2018-71.

[4] SEC Press Release (Oct. 2, 2017), available at www.sec.gov/news/press-release/2017-186.

[5] SEC Press Release (Feb. 21, 2018), available at www.sec.gov/news/press-release/2018-22; the guidance itself can be found at www.sec.gov/rules/interp/2018/33-10459.pdf. The SEC provided in-depth guidance in this release on disclosure processes and considerations related to cybersecurity risks and incidents, and complements some of the points highlighted in the Section 21A report.

Gibson Dunn's lawyers are available to assist with any questions you may have regarding these issues. For further information, please contact the Gibson Dunn lawyer with whom you usually work in the firm's Securities Enforcement or Privacy, Cybersecurity and Consumer Protection practice groups, or the following authors:

Marc J. Fagel - San Francisco (+1 415-393-8332, mfagel@gibsondunn.com)
Alexander H. Southwell - New York (+1 212-351-3981, asouthwell@gibsondunn.com)

Please also feel free to contact the following practice leaders and members:

Securities Enforcement Group:

New York
Barry R. Goldsmith - Co-Chair (+1 212-351-2440, bgoldsmith@gibsondunn.com)
Mark K. Schonfeld - Co-Chair (+1 212-351-2433, mschonfeld@gibsondunn.com)
Reed Brodsky (+1 212-351-5334, rbrodsky@gibsondunn.com)
Joel M. Cohen (+1 212-351-2664, jcohen@gibsondunn.com)
Lee G. Dunst (+1 212-351-3824, ldunst@gibsondunn.com)
Laura Kathryn O'Boyle (+1 212-351-2304, loboyle@gibsondunn.com)
Alexander H. Southwell (+1 212-351-3981, asouthwell@gibsondunn.com)
Avi Weitzman (+1 212-351-2465, aweitzman@gibsondunn.com)
Lawrence J. Zweifach (+1 212-351-2625, lzweifach@gibsondunn.com)

Washington, D.C.
Richard W. Grime - Co-Chair (+1 202-955-8219, rgrime@gibsondunn.com)
Stephanie L. Brooker (+1 202-887-3502, sbrooker@gibsondunn.com)
Daniel P. Chung (+1 202-887-3729, dchung@gibsondunn.com)
Stuart F. Delery (+1 202-887-3650, sdelery@gibsondunn.com)
Patrick F. Stokes (+1 202-955-8504, pstokes@gibsondunn.com)
F. Joseph Warin (+1 202-887-3609, fwarin@gibsondunn.com)

San Francisco
Marc J. Fagel - Co-Chair (+1 415-393-8332, mfagel@gibsondunn.com)
Winston Y. Chan (+1 415-393-8362, wchan@gibsondunn.com)
Thad A. Davis (+1 415-393-8251, tdavis@gibsondunn.com)
Charles J. Stevens (+1 415-393-8391, cstevens@gibsondunn.com)
Michael Li-Ming Wong (+1 415-393-8234, mwong@gibsondunn.com)

Palo Alto
Paul J. Collins (+1 650-849-5309, pcollins@gibsondunn.com)
Benjamin B. Wagner (+1 650-849-5395, bwagner@gibsondunn.com)

Denver
Robert C. Blume (+1 303-298-5758, rblume@gibsondunn.com)
Monica K. Loseman (+1 303-298-5784, mloseman@gibsondunn.com)

Los Angeles
Michael M. Farhang (+1 213-229-7005, mfarhang@gibsondunn.com)
Douglas M. Fuchs (+1 213-229-7605, dfuchs@gibsondunn.com)

Privacy, Cybersecurity and Consumer Protection Group:

Alexander H. Southwell - Co-Chair, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
M. Sean Royall - Dallas (+1 214-698-3256, sroyall@gibsondunn.com)
Debra Wong Yang - Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Christopher Chorba - Los Angeles (+1 213-229-7396, cchorba@gibsondunn.com)
Richard H. Cunningham - Denver (+1 303-298-5752, rhcunningham@gibsondunn.com)
Howard S. Hogan - Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen - Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley - San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon - Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Shaalu Mehra - Palo Alto (+1 650-849-5282, smehra@gibsondunn.com)
Karl G. Nelson - Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner - Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong - San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)