COVINGTON

SEC Report Calls for Better Internal Accounting Controls for Cyber-Related Threats

October 29, 2018

Capital Markets and Securities

On October 16, 2018, the Securities and Exchange Commission (the "Commission") issued a Section 21(a) report of investigation (the "Report") warning public companies about the importance of assessing the likelihood of cyber-related threats when designing internal accounting controls. The Report described the Division of Enforcement's investigation of nine unidentified public companies that collectively suffered approximately $100 million in financial losses as a result of email scams. The Commission ultimately decided not to pursue enforcement actions against the nine companies as a result of the investigation, but instead issued the Report to caution public companies about the need to implement and maintain internal accounting controls that provide reasonable assurances that a company's assets will be protected from cyber-related fraud.

The Report

Section 21(a) of the Securities Exchange Act of 1934 (the "Exchange Act") authorizes the Commission to investigate, as it deems necessary, potential violations of the federal securities laws and subsequently issue a public report of investigation describing the facts and circumstances surrounding such investigations. The Commission issues reports of investigation under Section 21(a) infrequently, and, when used, the reports generally highlight matters of broad significance.[1]

The Report resulted from an investigation by the Division of Enforcement, in consultation with the Division of Corporation Finance and the Office of the Chief Accountant, into the internal accounting controls of nine public companies, across a broad range of industries, that were victims of cyber-related fraud. Specifically, the Commission considered whether the companies complied with the requirements of Section 13(b)(2)(B) of the Exchange Act, which requires

[1] Since 1996, the Commission has issued only 16 reports of investigation under Section 21(a) of the Exchange Act. These reports have covered topics such as (i) the treatment of digital tokens as securities, (ii) the use of social media to disseminate material information about a company, (iii) the obligations of public officials relating to secondary market disclosures about municipal securities and (iv) securities liability for false or misleading statements about provisions in material contracts.

public companies to devise and maintain internal accounting controls sufficient to provide reasonable assurances that "transactions are executed" and "access to assets is permitted" only in accordance with management's authorization.

The approximately $100 million of losses suffered by the nine public company victims were the result of so-called "business email compromises." The Report identified two specific types of email scams suffered by these companies.

- **Fake Corporate Executive Emails.** These were fraudulent emails from persons claiming to be corporate executives. They included
  - emails sent from fake corporate executive email domains and addresses and typically requested mid-level finance employees to wire large sums of money to foreign bank accounts for time-sensitive transactions; and
  - unsophisticated emails with spelling and grammatical errors making urgent and unusual requests.
- **Fake Vendors' Emails.** These emails came from perpetrators which hacked into actual vendors' accounts and sent fake invoices and illegitimate requests for payments that appeared to be for legitimate transactions.
  - The fraudulent emails were sent to employees from the perpetrators posing as vendors and convinced the employees to change legitimate vendor banking information, thereby resulting in payments made on outstanding invoices to foreign accounts controlled by the perpetrators rather than legitimate vendors.
  - The Report indicates that some fake vendor electronic communications, which seemed more legitimate than the fake corporate executive emails and resulted in payments made to the fake vendors, went unnoticed for an extended period of time and were only discovered when legitimate vendors inquired into delinquent bills.

The Report states that these cyber-related frauds succeeded because company personnel either failed to understand and follow their company's existing cybersecurity controls or failed to scrutinize the emails at issue. For example, in one instance, an employee in the accounting department did not follow the company's dual authorization requirement for wire payments and directed unqualified subordinates to initiate payments. In other instances, recipients of the fake emails did not ask any questions about the transactions referenced in the emails, even when the employees had no knowledge of the transactions and were asked to make multiple payments over many months.

The Commission emphasized that the cyber-related frauds which victimized the companies were not sophisticated in design or technology and had the companies implemented and followed reasonable internal controls, the companies would have been in the position to detect the frauds. Notwithstanding these failings, the Commission did not pursue enforcement actions and, instead, highlighted the risks surrounding cyber-related fraud. In doing so, the Commission has given companies a firm warning to implement and maintain appropriate internal accounting controls to ensure that company funds are transferred only with management's approval and according to policies and procedures set forth by management.

Commission Guidance on Cybersecurity Disclosure and Recent Commission Enforcement Actions

The Report is the latest pronouncement by the Commission regarding cybersecurity risks. As described in our earlier alert, in February 2018 the Commission issued guidance to assist public companies in evaluating their disclosure obligations about cyber-related risks and incidents. The Commission's February 2018 guidance described the importance of implementing comprehensive policies and procedures related to cybersecurity controls, including disclosure controls, and emphasized the need to have policies to guard against insiders trading on material non-public information about cyber-related risks and incidents.

Since providing its February 2018 guidance, the Commission has brought its first enforcement action against a public company relating to a cyber-related incident. In April 2018, the Commission announced a $35.0 million settlement with Yahoo! Inc. ("Yahoo") for alleged delays in Yahoo's public disclosure of a large-scale data breach.[2] The Commission found that Yahoo learned of a breach of its user database in 2014 that resulted in the theft of hundreds of millions of consumer usernames, passwords, birthdates and telephone numbers. Yahoo, however, did not disclose the incident until September 2016. According to the Commission, Yahoo did not have proper procedures in place to assess and elevate information about theft of user data, including how and where such breaches should be disclosed in Yahoo's public filings. The Commission's enforcement action against Yahoo was rooted in its finding that the company did not "maintain disclosure controls and procedures designed to ensure that reports from Yahoo's information security team raising actual incidents of the theft of user data, or the significant risk of theft of user data, were properly and timely assessed to determine how and where data breaches should be disclosed in Yahoo's public filings, including, but not limited to, in its risk factor disclosures or MD&A."[3]

More recently, in September 2018, the Commission brought an action against Voya Financial Advisors ("VFA"), a registered broker-dealer and investment adviser which experienced a cyber-attack that allegedly compromised the personal information of thousands of customers.[4] According to the Commission's settlement order, for a six-day period in April 2016, VFA suffered a data breach when its technical and customer support personnel were deceived into resetting the account credentials of three contractor representatives, after which the perpetrators were able to access a system containing the personally identifiable information of approximately 5,600 customers.[5] Based on its findings, the Commission determined that VFA's policies and

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

[3] See In the Matter of Altaba Inc., f.d.b.a Yahoo! Inc., Administrative Proceeding File No. 3-18448 (Apr. 24, 2018), available at https://www.sec.gov/litigation/admin/2018/33-10485.pdf.

[4] SEC Press Release (Sept. 26, 2018), available at https://www.sec.gov/news/press-release/2018-213.

[5] See In the Matter of Voya Financial Advisors, Inc., Administrative Proceeding File No. 3-18840 (Sept. 26, 2018), available at https://www.sec.gov/litigation/admin/2018/34-84288.pdf.

procedures were not reasonably designed to protect customer records and information.[6] The Commission also found that VFA did not have an identity theft prevention program that was adequately designed to detect, prevent, and mitigate identity theft in customer accounts, one which included reasonable policies and procedures to identify and detect relevant red flags for customer accounts, to respond appropriately to detected red flags and to ensure periodic updates to the program to reflect changes in risks to customers from identity theft.[7] In connection with its agreement to settle the Commission's proceeding, VFA agreed to engage a compliance consultant to oversee a review and enhancement of VFA's compliance policies and procedures for safeguarding of customer records and information and for prevention of customer identity theft. VFA also agreed to pay a penalty of $1.0 million.

Practical Considerations

Cybersecurity remains a high priority for the Commission. The Report, following on the recent enforcement actions noted above, sends another clear signal that public companies and other SEC regulated entities need to be fully equipped to identify and address cybersecurity risks. By issuing the Report in lieu of pursuing enforcement actions against nine corporate victims of cyber-fraud, the Commission underscored a broad mandate for public companies to calibrate their internal accounting controls to the current cyber-risk environment and assess and adjust policies and procedures accordingly.

As noted in the Report, companies are in the best position to develop internal accounting controls that account for their particular operational needs and risks in complying with Section 13(b)(2)(B). In performing this analysis, companies should evaluate the extent to which they consider cyber-related threats when devising and maintaining their internal accounting control systems. And, as stated in the Report, "[g]iven the prevalence and continued expansion of these attacks, issuers should be mindful of the risks that cyber-related frauds pose and consider, as appropriate, whether their internal accounting control systems are sufficient to provide reasonable assurances in safeguarding their assets from these risks." As part of this effort, companies should provide training to their personnel regarding their policies to prevent and detect cyber-fraud in order to ensure that control systems are operating as designed.

Companies should assume that the Commission is actively monitoring all areas related to cybersecurity, including corporate disclosures of cyber-related incidents and also whether companies have established policies, procedures, and internal controls in place to ensure cyber-related incidents are prevented. Given that assumption, public companies should take prompt steps to assess and, if appropriate, improve internal accounting controls, disclosure

---

[6] See 17 C.F.R. §248.30(a)(the "Safeguards Rule"). The Safeguards Rule requires every registered broker-dealer and investment adviser to adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information.

[7] See 17 C.F.R. §248.201 (the "Identity Theft Red Flags Rule"). The Identity Theft Red Flags Rule requires certain financial institutions, including registered broker-dealers and investment advisers, to develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identify theft in connection with the opening of a customer account or any existing customer account.

controls, and cyber-related policies and procedures to address the risk of cyber-related incidents.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Capital Markets and Securities practice:

David Martin (co-author)	+1 202 662 5128	dmartin@cov.com
David Engvall (co-author)	+1 202 662 5307	dengvall@cov.com
Donald Murray	+1 212 841 1101	dmurray@cov.com
Eric Blanchard	+1 212 841 1111	eblanchard@cov.com
Kerry Burke (co-author)	+1 202 662 5297	kburke@cov.com
Gerald Hodgkins (co-author)	+1 202 662 5263	ghodgkins@cov.com
Brian Rosenzweig	+1 212 841 1108	brosenzweig@cov.com
Matt Franker (co-author)	+1 202 662 5895	mfranker@cov.com
Reid Hooper (co-author)	+1 202 662 5984	rhooper@cov.com