October 17, 2018

SEC Issues Report of Investigation on Cyber-Related Frauds Perpetrated Against Public Companies

Public Companies Should Implement Sufficient Internal Controls to Avoid Becoming Victims of Cyber-Related Frauds and to Comply With the Exchange Act

SUMMARY

On October 16, the SEC issued a report on an investigation into whether nine public issuers that were victims of cyber-related frauds may have violated Sections 13(b)(2)(B)(i) and (iii) of the Exchange Act by failing to have a sufficient system of internal accounting controls to provide reasonable assurances that those frauds were detected and prevented.

The issuers, which the SEC stated represent a variety of industries, were victims of two types of "business email compromise" scams that resulted in mostly unrecovered losses ranging from $1 million to over $45 million.

While the SEC determined not to pursue enforcement actions against the issuers under investigation, it issued its report of investigation to make issuers aware that the cyber-related threats exist and concluded that all companies should reassess the sufficiency not only of existing internal controls, but also of policies and procedures that ensure employee compliance with controls.

DISCUSSION

The Securities Exchange Act of 1934 (the "Exchange Act") requires public companies to maintain internal accounting controls sufficient to provide reasonable assurances that transactions are executed in accordance with and access to company assets is only permitted with "management's general or

specific authorization."[1] In the course of its investigation, the Securities and Exchange Commission (the "SEC") sought to determine whether the controls of nine public issuers were sufficient to comply with these obligations.[2]

Each issuer was the victim of one of two types of scams known as "business email compromises." The first type involved perpetrators who used spoofed email addresses to pose as company executives in emails sent to company finance personnel. In the emails, the perpetrators directed the finance personnel to work with a purported outside attorney identified in the email, who then directed them to cause large sums of money to be transferred to foreign bank accounts controlled by the perpetrators. The emails generally used real law firm and attorney names, but the contact details in fact connected the personnel with an impersonator and co-conspirator. The emails also described purported time-sensitive requests, mentioned the need for confidentiality of the transfers, provided minimal details, and sometimes falsely implied that the transactions involved government oversight, including the coordination or supervision of the SEC. Even though all of the issuers did business internationally, the emails often described foreign transactions that were out of the ordinary for the particular issuer. The email recipients were typically mid-level employees who ordinarily would have had no involvement in the purported transactions, and rarely communicated with the executives being spoofed.

The second type of scam involved perpetrators who hacked into the email accounts of issuers' vendors. Posing as a vendor, these perpetrators inserted illegitimate payment requests and payment processing details into electronic communications for otherwise legitimate transaction requests. The perpetrators corresponded with issuers' unsuspecting procurement personnel to obtain information about purchase orders and invoices. The perpetrators then requested that the procurement personnel initiate changes to the vendors' banking information, attaching doctored invoices reflecting the new, fraudulent account information, and the procurement personnel relayed that information to accounting personnel responsible for maintaining vendor data. As a result, the issuers made payments on outstanding invoices to foreign accounts controlled by the perpetrators.

Many issuers remained unaware of these schemes, some of which continued over significant periods of time, until the schemes were uncovered as a result of third-party actions, including detection by a foreign bank or law enforcement agency, or by a vendor who complained of non-payment of invoices. The SEC noted that the schemes were often successful largely because employees either did not understand or did not follow the issuers' internal control procedures. As a result, the issuers as a group lost and did not recover nearly $100 million, even though they had specific information about the foreign bank accounts that received the wired funds.

Notably, even with the relevant wire transfer confirmations, money transferred in these schemes may be difficult or impossible to recover by U.S. issuers or law enforcement. The money is typically transferred and dissipated quickly through foreign accounts in the names of shell corporations or false identities

created by the perpetrators. Further, the perpetrators often transfer the funds to foreign jurisdictions that are unlikely to cooperate with U.S. law enforcement requests for evidence or asset recovery.

OBSERVATIONS AND IMPLICATIONS

The SEC noted that email scams like the ones investigated here have caused business losses of over $5 billion since 2013, which according to the Federal Bureau of Investigation ("FBI") is greater than losses caused by any other type of cyber-related crime.[3] The FBI has also found that the threat of email scam losses has grown over time.[4] As such, the SEC strongly emphasized the importance of maintaining internal accounting controls that are sufficient to provide reasonable assurances that financial transactions are authorized by management.[5] Although the SEC determined not to pursue enforcement action in these matters, the report of investigation makes it clear that the SEC expects issuers to calibrate their internal controls to address the risks of cyber-related frauds. Because the scams commonly targeted "human vulnerabilities that rendered the control environment ineffective,"[6] the SEC also instructed companies to view employee training as a critical aspect of control implementation. All companies are advised to re-assess the sufficiency of internal accounting controls, especially those relating to foreign transactions, as well as the completeness of employee education protocols.

* * *

ENDNOTES

1 15 U.S.C. §§ 78m(b)(2)(B)(i), (iii).

2 *See* SEC, 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) ("SEC Report"). *See also* SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, at 18 (Feb. 21, 2018) ("[c]ybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with the federal securities laws.").

3 *See* FBI, 2017 Internet Crime Report at 12, 21, available at https://pdf.ic3.gov/2017_IC3Report.pdf (May 7, 2018).

4 *See* FBI, Public Service Announcement: Business E-Mail Compromise: E-Mail Account Compromise: The 5 Billion Dollar Scam (May 4, 2017) ("The BEC/EAC scam continues to grow, evolve, and target small, medium, and large businesses. Between January 2015 and December 2016, there was a 2,370% increase in identified exposed losses.").

5 The degree of assurance necessary is one "as would satisfy prudent officials in the conduct of their own affairs." 15 U.S.C. § 78m(b)(7).

6 SEC Report at 5.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York

Mehdi Ansari	+1-212-558-4314	ansarim@sullcrom.com
Robert E. Buckholz	+1-212-558-3876	buckholzr@sullcrom.com
Catherine M. Clarkin	+1-212-558-4175	clarkinc@sullcrom.com
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Donald R. Crawshaw	+1-212-558-4016	crawshawd@sullcrom.com
Robert W. Downes	+1-212-558-4312	downesr@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
William G. Farrar	+1-212-558-4940	farrarw@sullcrom.com
Jared M. Fishman	+1-212-558-1689	fishmanj@sullcrom.com
Nicole Friedlander	+1-212-558-4332	friedlandern@sullcrom.com
John P. Mead	+1-212-558-3764	meadj@sullcrom.com
Mark J. Menting	+1-212-558-4859	mentingm@sullcrom.com
Scott D. Miller	+1-212-558-3109	millersc@sullcrom.com
Nader A. Mousavi	+1-212-558-1624	mousavin@sullcrom.com
Richard A. Pollack	+1-212-558-3497	pollackr@sullcrom.com
Robert W. Reeder III	+1-212-558-3755	reederr@sullcrom.com
Melissa Sawyer	+1-212-558-4243	sawyerm@sullcrom.com
James M. Shea Jr.	+1-212-558-4924	sheaj@sullcrom.com
William D. Torchiana	+1-212-558-4056	torchianaw@sullcrom.com
Marc Trevino	+1-212-558-4239	trevinom@sullcrom.com
Benjamin H. Weiner	+1-212-558-7861	weinerb@sullcrom.com

Washington, D.C.		
Eric J. Kadel, Jr.	+1-202-956-7640	kadelej@sullcrom.com
Robert S. Risoleo	+1-202-956-7510	risoleor@sullcrom.com
Los Angeles		
Patrick S. Brown	+1-310-712-6603	brownp@sullcrom.com
Alison S. Ressler	+1-310-712-6630	resslera@sullcrom.com
Palo Alto		
Scott D. Miller	+1-650-461-5620	millersc@sullcrom.com
Nader A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com
Sarah P. Payne	+1-650-461-5669	paynesa@sullcrom.com
John L. Savva	+1-650-461-5610	savvaj@sullcrom.com
London		
Kathryn A. Campbell	+44-20-7959-8580	campbellk@sullcrom.com
Richard A. Pollack	+44-20-7959-8404	pollackr@sullcrom.com
David Rockwell	+44-20-7959-8575	rockwelld@sullcrom.com
Paris		
William D. Torchiana	+33-1-7304-5890	torchianaw@sullcrom.com
Frankfurt		
Krystian Czerniecki	+49-69-4272-5525	czernieckik@sullcrom.com
Melbourne		
Robert Chu	+61-3-9635-1506	chur@sullcrom.com
Sydney		
Waldo D. Jones, Jr.	+61-2-8227-6702	jonesw@sullcrom.com
Tokyo		
Izumi Akai	+81-3-3213-6145	akaii@sullcrom.com
Keiji Hatano	+81-3-3213-6171	hatanok@sullcrom.com
Hong Kong		
Garth W. Bray	+852-2826-8691	brayg@sullcrom.com
Chun Wei	+852-2826-8666	weic@sullcrom.com