SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 84429 / October 16, 2018

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

I. INTRODUCTION

The United States Securities and Exchange Commission's ("Commission") Division of Enforcement ("Division"), in consultation with the Division of Corporation Finance and the Office of the Chief Accountant, investigated whether certain public issuers that were victims of cyber-related frauds may have violated the federal securities laws by failing to have a sufficient system of internal accounting controls.

As discussed more fully below, the issuers—a group that spans numerous industries—each lost millions of dollars as a result of cyber-related frauds. In those frauds, company personnel received spoofed or otherwise compromised electronic communications purporting to be from a company executive or vendor, causing the personnel to wire large sums or pay invoices to accounts controlled by the perpetrators of the scheme. Spoofed or manipulated electronic communications are an increasingly familiar and pervasive problem, exposing individuals and companies, including public companies, particularly those that engage in transactions with foreign customers or suppliers, to significant risks and financial losses. The Federal Bureau of Investigation recently estimated that these so-called "business email compromises" had caused over $5 billion in losses since 2013, with an additional $675 million in adjusted losses in 2017—the highest estimated out-of-pocket losses from any class of cyber-facilitated crime during this period.[1]

In connection with the investigation, the Commission considered whether the issuers complied with the requirements of Sections 13(b)(2)(B)(i) and (iii) of the Securities Exchange

[1] FBI, *2017 Internet Crime Report* at 12, 21 (issued May 7, 2018) *available at* https://pdf.ic3.gov/2017_IC3Report.pdf ("FBI Internet Crime Report") (the FBI defines business email comprise as "a sophisticated scam targeting businesses that often work with foreign suppliers and/or businesses and regularly perform wire transfer payments," and includes frauds impacting both private and public companies); FBI, *Public Service Announcement: E-Mail Account Compromise the 5 Billion Dollar Scam* (May 4, 2017), *available at* https://www.ic3.gov/media/2017/170504.aspx ("FBI PSA"); *see also* Proofpoint, *2017 Email Fraud Threat Report* at 3 (Feb. 12, 2018) *available at* https://www.proofpoint.com/sites/default/files/pfpt-us-tr-email-fraud-yir-180212.pdf (finding that by the fourth quarter of 2017, nearly 89% of all organizations were targeted by at least one attack, over a 13% increase from the fourth quarter of 2016).

Act of 1934 ("Exchange Act").[2] Those provisions require certain 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 authorization.[3] As the Senate emphasized over four decades ago when passing these provisions, "[a] fundamental aspect of management's stewardship responsibility is to provide shareholders with reasonable assurances that the business is adequately controlled."[4] While the cyber-related threats posed to issuers' assets are relatively new, the expectation that issuers will have sufficient internal accounting controls and that those controls will be reviewed and updated as circumstances warrant is not.

The Commission has determined not to pursue an enforcement action in these matters based on the conduct and activities of these public issuers that are known to the Commission at this time. The Commission, however, deems it appropriate and in the public interest to issue this Report of Investigation ("Report") pursuant to Section 21(a) of the Exchange Act 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. Having sufficient internal accounting controls plays an important role in an issuer's risk management approach to external cyber-related threats, and, ultimately, in the protection of investors.

II. INVESTIGATIONS

The Division's investigation focused on the internal accounting controls of nine issuers that were victims of one of two variants of schemes involving spoofed or compromised electronic communications from persons purporting to be company executives or vendors. The issuers covered a range of sectors including technology, machinery, real estate, energy, financial, and consumer goods, reflecting the reality that every type of business is a potential target of

[2] 15 U.S.C. § 78m(b)(2)(B)(i) & (iii).

[3] The issuers with these Section 13(b)(2) obligations are those that have a class of securities registered with the Commission under Section 12 of the Exchange Act or that must file reports with the Commission under Section 15(d) of the Exchange Act. 15 U.S.C. § 78m(b)(6). Also the level of reasonable assurances required under these provisions is defined as such "degree of assurance as would satisfy prudent officials in the conduct of their own affairs." 15 U.S.C. § 78m(b)(7).

[4] S. Rep. No. 95-114, at 8 (1977) ("1977 Senate Report"); *see also Promotion of the Reliability of Financial Information and Prevention of the Concealment of Questionable or Illegal Corporate Payments and Practices*, Exchange Act Release No. 15570, at 6 (Feb. 15, 1979) (adopting release) ("An equally important objective of the new law . . . is the goal of corporate accountability.").

cyber-related fraud.[5] At the time of the cyberscams, each issuer had substantial annual revenues and had securities listed on a national securities exchange.

Each of the nine issuers lost at least $1 million; two lost more than $30 million. In total, the nine issuers lost nearly $100 million to the perpetrators, almost all of which was never recovered. Some of the investigated issuers were victims of protracted schemes that were only uncovered as a result of third-party actions, such as through detection by a foreign bank or law enforcement agency. Indeed, one company made 14 wire payments requested by the fake executive over the course of several weeks—resulting in over $45 million in losses—before the fraud was uncovered by an alert from a foreign bank. Another of the issuers paid eight invoices totaling $1.5 million over several months in response to a vendor's manipulated electronic documentation for a banking change; the fraud was only discovered when the real vendor complained about past due invoices.

Emails from Fake Executives. The first type of business email compromise the Division reviewed involved emails from persons not affiliated with the company purporting to be company executives. In these situations, the perpetrators of the scheme emailed company finance personnel, using spoofed email domains and addresses of an executive (typically the CEO) so that it appeared, at least superficially, as if the email were legitimate. In all of the frauds, the spoofed email directed the companies' finance personnel to work with a purported outside attorney identified in the email, who then directed the companies' finance personnel to cause large wire transfers to foreign bank accounts controlled by the perpetrators. The perpetrators used real law firm and attorney names, and legal services-sounding email domains like "consultant.com," but the contact details connected company personnel with an impersonator and co-conspirator. These were not sophisticated frauds in general design or the use of technology. In fact, from a technological perspective they only required creating an email address to mimic the executive's address. Each of the schemes had some common elements:

- The spoofed emails described time-sensitive transactions or "deals" that needed to be completed within days, and emphasized the need for secrecy from other company employees. They sometimes implied some level of government oversight, such as one fraudulent email claiming the purported transaction was "in coordination with and under the supervision of the SEC."

- The spoofed emails stated that the funds requested were necessary for foreign transactions or acquisitions, and directed the wire transfers to foreign banks and beneficiaries. Although all of the issuers had some foreign operations, these purported foreign transactions would have been unusual for most of them. The emails also provided minimal details about the transactions.

[5] The Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy* at 6 (Feb. 2018), *available at* https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf ("Council of Economic Advisers Report") ("That said, every firm is a potential target, independent of its age, size, sector, location, or employee composition.").

- The spoofed emails typically were sent to midlevel personnel, who were not generally responsible or involved in the purported transactions (and who rarely communicated with the executives being spoofed). The emails also often included spelling and grammatical errors.

Emails from Fake Vendors. The second type of cyber-related fraud involved electronic communications impersonating the issuers' vendors. This form of scam was more technologically sophisticated than the spoofed executive emails because, in the instances the Division reviewed, the schemes involved intrusions into the email accounts of issuers' foreign vendors. After hacking the existing vendors' email accounts, the perpetrators inserted illegitimate requests for payments (and payment processing details) into electronic communications for otherwise legitimate transaction requests. The perpetrators of these scams also corresponded with unwitting issuer personnel responsible for procuring goods from the vendors so that they could gain access to information about actual purchase orders and invoices. The perpetrators then requested that the issuer personnel initiate changes to the vendors' banking information, and attached doctored invoices reflecting the new, fraudulent account information. The issuer personnel responsible for procurement 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 impersonator rather than the accounts of the real vendors.

Unlike the fake executive scams, the spoofed vendor emails had fewer indicia of illegitimacy or red flags. In fact, several victims only learned of the scam when the real vendor raised concerns about nonpayment on outstanding invoices. Because vendors often afford issuers months before considering a payment delinquent, the scams, in certain circumstances, were able to continue for an extended period of time.

III. DISCUSSION

The Commission recently emphasized that "cybersecurity presents ongoing risks and threats to our capital markets and to companies operating in all industries, including public companies regulated by the Commission."[6] Accordingly, the Commission Statement and Guidance on Public Company Cybersecurity Disclosures advised such public companies that "[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."[7]

---

[6] *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, at 2 (Feb. 21, 2018), *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf ("Commission Statement on Cybersecurity Disclosures"); *see also* World Economic Forum, *The Global Risks Report 2018* at 6 (Jan. 17, 2018), *available at* http://www3.weforum.org/docs/WEF_GRR18_Report.pdf ("World Economic Forum Report") (identifying cyberattacks as one of the top five global risks in terms of likelihood).

[7] Commission Statement on Cybersecurity Disclosures at 18.

In light of the risks associated with today's ever expanding digital interconnectedness, public companies should pay particular attention to the obligations imposed by Section 13(b)(2)(B) to devise and maintain internal accounting controls that reasonably safeguard company and, ultimately, investor assets from cyber-related frauds. More specifically, Section 13(b)(2)(B)(i) and (iii) require certain issuers to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that (i) transactions are executed in accordance with management's general or specific authorization," and that "(iii) access to assets is permitted only in accordance with management's general or specific authorization."[8] As the Senate underscored when these provisions were passed, "[t]he expected benefits from the conscientious discharge of these responsibilities are of basic importance to investors and the maintenance of the integrity of our capital market system."[9]

Virtually all economic activities now take place through digital technology and electronic communication, leaving business transactions and assets susceptible to a variety of cyber-related threats.[10] This is a growing global problem, and cyberscams like the ones described above that target an issuer's assets are an ever-increasing part of the cybersecurity threats faced by a wide variety of businesses, including issuers with Section 13(b)(2)(B) obligations.[11] The financial and other impacts of these frauds can be significant, as the instances described above attest.

As noted above, these frauds were not sophisticated in design or the use of technology; instead, they relied on technology to search for both weaknesses in policies and procedures and human vulnerabilities that rendered the control environment ineffective. Having internal accounting control systems that factor in such cyber-related threats, and related human vulnerabilities, may be vital to maintaining a sufficient accounting control environment and safeguarding assets.

These examples underscore the importance of devising and maintaining a system of internal accounting controls 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 issuers here, for instance, had procedures that required

---

[8] 15 U.S.C. § 78m(b)(2)(B)(i) & (iii).

[9] 1977 Senate Report at 8.

[10] *See, e.g.*, World Economic Forum Report at 14 ("Attacks are increasing, both in prevalence and disruptive potential.").

[11] *See* FBI Internet Crime Report at 12 ("In 2017, the IC3 received 15,690 BEC/EAC complaints with adjusted losses of over $675 million"); FBI PSA ("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."). These figures include losses sustained by private or public companies, and so are not limited to those with securities registered under Section 12 of the Exchange Act or those that must file reports under Section 15(d) of the Exchange Act.

certain levels of authorization for payment requests, management approval for outgoing wires, and verification of any changes to vendor data. Yet they still became victims of these attacks. The existing controls could be (and were) interpreted by the company's personnel to mean that the (ultimately compromised) electronic communications were, standing alone, sufficient to process significant wire transfers or changes to vendor banking data. To that end, after falling victim to these frauds, each of the issuers sought to enhance their payment authorization procedures, and verification requirements for vendor information changes. Moreover, as noted above, many of these issuers only learned of the fraud as a result of third-party notices, such as from law enforcement or foreign banks. Thereafter, these issuers took steps to bolster their account reconciliation procedures and outgoing payment notification processes to aid detection of payments resulting from fraud.[12]

Systems of internal accounting controls, by their nature, depend also on the personnel that implement, maintain, and follow them. In the context of the business email compromises the Division reviewed, the frauds succeeded, 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. For example, in one matter, the accounting employee who received the spoofed email did not follow the company's dual-authorization requirement for wire payments, directing unqualified subordinates to sign-off on the wires. In another, the accounting employee misinterpreted the company's authorization matrix as giving him approval authority at a level reserved for the CFO. And there were numerous examples where the recipients of the fraudulent communications asked no questions about the nature of the supposed transactions, even where such transactions were clearly outside of the recipient employee's domain and even where the employee was asked to make multiple payments over days and even weeks. In two instances the targeted recipients were themselves executive-level employees—chief accounting officers—who initiated payments in response to fake executive emails. To this end, while most of the issuers had some form of training regarding controls and information technology in place prior to the scams, all of them enhanced their training of responsible personnel about relevant threats, as well as about pertinent policies and procedures following the frauds.

IV. CONCLUSION

By this report, the Commission 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. What is clear, however, is 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.

---

[12] *See, e.g.*, *Statement of Policy Regarding the Foreign Corrupt Practices Act of 1977*, 46 Fed. Reg. 11544, at 11547 (Jan. 29, 1981) ("[W]hen discovery and correction expeditiously follow, no failing in the company's internal accounting system would have existed. To the contrary, routine discovery and correction would evidence its effectiveness.").

Ultimately, issuers themselves 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).[13] In performing this analysis, issuers should evaluate to what extent they should consider cyber-related threats when devising and maintaining their internal accounting control systems. Given 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.

[13] *See* 1977 Senate Report at 8 (". . . management must exercise judgment in determining the steps to be taken, and the cost incurred, in giving assurance that the objectives expressed, will be achieved."); Council of Economic Advisers Report at 45 ("Private firms are ultimately in the best position to figure out the most appropriate sector- and firm-specific cybersecurity practices.").