John W. White
+1-212-474-1732
jwhite@cravath.com

Hon. Katherine B. Forrest (Fmr.)
+1-212-474-1151
kforrest@cravath.com

Rachel G. Skaistis
+1-212-474-1934
rskaistis@cravath.com

John D. Buretta
+1-212-474-1260
jburetta@cravath.com

Benjamin Gruenstein
+1-212-474-1080
bgruenstein@cravath.com

David M. Stuart
+1-212-474-1519
dstuart@cravath.com

Evan Norris
+1-212-474-1524
enorris@cravath.com

U.S. Securities and Exchange Commission Cautions Public Companies on Risks Arising from Cyber-Related Frauds

October 24, 2018

Last week, the U.S. Securities and Exchange Commission issued a rare investigative report under Section 21(a) of the Securities Exchange Act cautioning public companies about the importance of considering cyber-related fraud threats when devising and maintaining their internal accounting controls.[1] The report followed the conclusion of the SEC's investigation of nine public issuers that had been victims of business email compromises, a type of cyber-related fraud in which company employees receive fraudulent electronic communications purporting to be from a senior executive or vendor, inducing the employee to wire large sums to accounts controlled by the perpetrators of the scheme.

While the Commission announced it would not pursue enforcement actions against the nine companies under investigation, it issued the report to put others on notice that—going forward—the failure to have a system of internal accounting controls sufficiently calibrated to the risks posed by such cyber-related frauds may result in a violation of federal securities laws. In the SEC's view, "[w]hile 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 SEC INVESTIGATION

The investigation that led to the issuance of the report was conducted by the SEC's Division of Enforcement, in consultation with the Division of Corporation Finance and the Office of the Chief Accountant. The investigation examined companies in a range of industry sectors, including technology, machinery, real estate, energy, financial and consumer goods—reflecting, in the words of the Commission, "the reality that every type of business is a potential target of cyber-related fraud".

The investigation focused on two categories of business email compromise fraud schemes. First, it looked at schemes involving emails sent by individuals not affiliated with the victim issuer who purported to be company executives—what the SEC

---

[1] 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, Securities Exchange Act Release No. 84429 (Oct. 16, 2018). In a related vein, the SEC also last week announced the launch of FinHub, a strategic new hub for innovation and financial technology to enhance investor protection in the era of new technological advancements. See SEC Launches New Strategic Hub for Innovation and Financial Technology, Press Release 2018-240 (Oct. 18, 2018).

termed "Emails from Fake Executives". Second, it examined schemes involving emails sent by individuals impersonating the issuers' vendors—"Emails from Fake Vendors". As further detailed below, the schemes resulted in losses to the victim issuers between $1 million and $45 million each, totaling nearly $100 million, almost none of which was recovered.

Emails from "Fake Executives"

As described in the SEC's report, the first type of scheme involves a relatively unsophisticated cyber fraud, in which perpetrators create an email account that allows them to impersonate a real executive at the company, usually the CEO. Such "spoofed" emails typically instruct a member of the victim company's finance department to coordinate with a purported outside attorney (in reality, another participant in the scheme) who then directs the unwitting employee to transfer a sum of money to the fake executive's account. Perpetrators often use real law firm and attorney names, or plausible-sounding email domains like "consultant.com", to make the ruse appear legitimate. Two of the schemes under investigation targeted the victim companies' chief accounting officers, both of whom initiated payments in response to emails from fake executives. One of the schemes involved a victim company that lost over $45 million transferred in 14 wire payments made over the course of several weeks, which might have gone undetected even longer had the fraud not been identified by a foreign bank.

Emails from "Fake Vendors"

The second type of scheme described by the SEC involves a more technologically advanced impersonation of a company's vendor. In the "spoofed vendor emails" scheme, perpetrators typically request that the company update the vendor's stored banking information with the details of a fraudulent account under the perpetrators' control. The schemes investigated by the Enforcement Division were particularly difficult to detect because they involved intrusions into the email accounts of the victim issuers' foreign vendors followed by insertions of "illegitimate requests for payments (and payment processing details) into electronic communications for otherwise legitimate transaction requests". With "fewer indicia of illegitimacy or red flags", many of these schemes lasted for months and were only discovered when the legitimate vendor raised concerns over delinquent payments or law enforcement intervened.

DISCUSSION

The SEC only rarely uses its power to issue investigative reports to make public its findings from investigations without an enforcement action for the purpose of providing guidance on a novel securities law issue. This report is intended to put companies on notice that if they experience failures of the type described in the report, they may fail to satisfy the internal controls requirements under the federal securities laws and be charged in an enforcement action. "The Commission . . . deems it appropriate and in the public interest to issue this [r]eport . . . to make issuers and other market participants aware that these cyber-related threats of spoofed or manipulated communications exist and should be considered when devising and maintaining a system of internal accounting controls as required by the federal securities laws". In particular, the Commission made clear that companies "should pay particular attention to" Sections 13(b)(2)(B)(i) and (iii) of the Exchange Act, which require certain issuers to devise and maintain internal accounting controls that "reasonably safeguard company and, ultimately, investor assets from cyber-related frauds".

The SEC further emphasized that while the nine issuers that had been under investigation all had some kind of internal accounting controls in place—such as procedures requiring certain levels of authorization for payment requests, account reconciliation procedures, outgoing payment notification processes or some form of employee cyber training—none effectively prevented these attacks. In each case, company personnel bypassed internal controls, either because they did not understand them sufficiently or did not recognize the red flags, thereby paving the way for a successful cyber-related attack.

Companies would do well to heed the SEC's admonishment that "[h]aving 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" as required by Section 13(b)(2)(B) (emphasis added).

CONCLUSION

The FBI estimates that losses resulting from business email compromise schemes have totaled over $5 billion in the last five years, with an additional $675 million in adjusted losses last year alone—"the highest estimated out-of-pocket losses from any class of cyber-facilitated crime during this period". While the SEC does not view every issuer that falls victim to a cyber-related fraud to be, by extension, in violation of federal securities laws, prudent issuers will now want to ensure that they are in a position to reassess regularly their existing enterprise-wide risk management systems and calibrate them to mitigate the risk of these increasingly common types of cyber-related frauds.

Last week's report continues the steady pace of pronouncements relating to cybersecurity that the SEC began in earnest last year when it announced its creation of a Cyber Unit.[2] Over a dozen enforcement actions relating to improper trading as a result of hacking and fraud relating to cryptocurrencies and initial coin offerings have followed, and in February 2018 the Commission issued interpretative guidance addressing the importance of timely public disclosures concerning cybersecurity risks and incidents.[3] The new report goes a step further in articulating the Commission's view on the types of controls and trainings companies should consider to prevent particular types of cyber incidents from occurring.

Further pronouncements are likely to follow in the weeks and months ahead. In the meantime, public companies in particular should take last week's report seriously and carefully review their internal controls —and continue to do so on a regular basis—to determine whether improvements are necessary.

New York
Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
+1-212-474-1000

London
CityPoint
One Ropemaker Street
London EC2Y 9HR
+44-20-7453-1000

www.cravath.com

[2] SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors, Press Release 2017-176 (Sept. 25, 2017).

[3] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Securities Act Release No. 33-10459, Securities Exchange Act Release No. 34-82746, 83 FR 8166 (effective Feb. 26, 2018). See also our client alert "U.S. Securities and Exchange Commission 2019 Budget Request Prioritizes Cybersecurity Enforcement and Management of Internal Cybersecurity Risk" (Feb. 14, 2018), https://www.cravath.com/files/Uploads/Documents/Publications/3702117_1.pdf.