The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 31562

January 16, 2019

SEC Brings Charges Related to 2016 EDGAR Hacking Case

[31562]

January 16, 2019 TO: ICI Members
Chief Compliance Officer Committee
Chief Information Security Officer Advisory Committee
Technology Committee SUBJECTS: Cybersecurity
Litigation & Enforcement RE: SEC Brings Charges Related to 2016 EDGAR Hacking Case

As you may recall, in September 2017, SEC Chairman Clayton issued a public statement on cybersecurity.[1] This statement included the first public disclosure that, in 2016, the SEC's EDGAR system had been breached. As disclosed in the statement:

> In August 2017, the Commission learned that an incident previously detected in 2016 may have provided the basis for illicit gain through trading. Specifically, a software vulnerability in the test filing component of the Commission's EDGAR system, which was patched promptly after discovery, was exploited and resulted in access to nonpublic information. It is believed the intrusion did not result in unauthorized access to personally identifiable information, jeopardize the operations of the Commission, or result in systemic risk. An internal investigation was commenced immediately at the direction of the Chairman. ;

Yesterday, the SEC filed a civil action against the persons who were behind the 2016 hacking.[2] The allegations in the SEC's Complaint are briefly summarized below. The Complaint seeks a jury trial and the imposition of sanctions, including an injunction, civil monetary penalties, and the disgorgement of ill-gotten gains with interest.

The Defendants

The Complaint names nine Defendants and four "relief defendants."[3] Of the nine Defendants, one is referred to in the Complaint as the "Hacker Defendant." The Hacker Defendant is a 27-year old Ukrainian who conducted the hacking activity that was the basis for the Complaint. Of the remaining eight Defendants, three are trading firms and six are individuals who traded on the hacked information. The Defendants involved in trading on information that was exfiltrated through hacking compensated the Hacker Defendant for the information he provided to them.

The Defendants' Newswire Hacking

According to the Complaint, the Defendants' breach of the SEC's EDGAR system in 2016 followed their breach of newswires that had occurred from 2010-2015. Through the hack of the newswires' computer systems, the Defendants accessed over 100,000 draft press releases before they were published. They were able to monetize this information by trading on it prior to it becoming public. The Defendants' illegal access to the newswire services was disrupted in 2015 and they were civilly and criminally charged with illegal activity. These cases remain pending.[4]

The Defendants' EDGAR Hacking

Following the cessation of the Defendants' newswire hacking, they targeted the SEC's EDGAR system as a new source of nonpublic information that could be used for securities trading. As explained in the Complaint, prior to making information public through an EDGAR filing, filers may submit "test filings" to EDGAR. "Test filings are draft versions of EDGAR filings that are meant to ensure that an EDGAR filing is in the correct format, free from errors, and will be accepted for filing by EDGAR. Test filings are not meant for public dissemination and are not publicly available."[5] In the spring of 2016, the Hacker Defendant launched several concurrent efforts to surreptitiously exfiltrate from the SEC's EDGAR servers material nonpublic information that could be used to profitably trade securities. These efforts included each of the following:

- Using hacking techniques to circumvent pages of the EDGAR system that required users to login with their credentials to access user identification information;
- Misrepresenting himself as an authorized EDGAR filer and accessing nonpublic test filings within EDGAR system;
- Using numerous aliases to conceal his control of an IP address used in the EDGAR hack and a related domain used in previous hacks of newswire services; and
- Inducing SEC computer users to open documents containing malware sent via spoofed, phishing emails that falsely represented that they had been sent by SEC security personnel.[6]

The Defendants' email spoofs that contained malware-infected documents and their phishing activities "successfully infected several SEC computer workstations in an attempt to obtain material nonpublic information."[7]

According to the Complaint, after determining that the material nonpublic information obtained by hacking EDGAR could be used to trade profitably, the Hacker Defendant began to deploy a server, referred to in the Complaint as an "Exfiltration Machine," using a program to perform on an automated basis the deceptive conduct that he had been performing manually. The Complaint notes that the Exfiltration Machine enabled the Hacker Defendant "to obtain hacked test filings on a greater scale."[8] To accommodate increased trading on this information, more traders were used to monetize the exfiltrated information.

Through his efforts, the Hacker Defendant was able to penetrate the EDGAR computer network to access certain nonpublic return copies of EDGAR test filings. His efforts began on or about May 3, 2016 and continued until at least October 20, 2016. In October 2016, the SEC's IT personnel patched EDGAR software in response to a detected attack on the system, which also had the effect of preventing the Hacker Defendant from accessing test filings. Notwithstanding this, the Hacker Defendant continued to attempt to compromise EDGAR into early 2017, though none of these efforts appear to have been successful according to the Complaint. The Trader Defendants, in turn, were able to trade on the

nonpublic information obtained by the Hacker Defendant and all Defendants profited from this scheme, whether the exfiltrated information was positive or negative. Their profits from this activity exceeded $4.1 million.

The Complaint includes a charge showing how the Defendant Traders, when they conducted trades based on public information, tended to lose money on their trades. By comparison, when they traded based on information exfiltrated from EDGAR, they made profitable trades.[9]

The Defendants' Violations of Law

Based upon the above conduct, the Complaint alleges that the Defendants violated the antifraud provisions of: Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5 thereunder; Section 17(a) of the Securities Act of 1933; and the aiding and abetting provisions of Section 10(b) of the Exchange Act and Rule 10b-5 thereunder and Section 17(a) of the Securities Act.

Tamara K. Salmon
Associate General Counsel

endnotes

[1] The Chairman's statement is available at: https://www.sec.gov/news/press-release/2017-170.

[2] *See U.S. Securities and Exchange Commission v. Oleksandr Ieremenko, et al.,* District of New Jersey, Civil Action No. 19-cv-505, (January 15, 2019) (the "Complaint"), which is available at: https://www.sec.gov/litigation/litreleases/2018/lr24193.htm. The press release the SEC issued about this action is available at: https://www.sec.gov/news/press-release/2019-1. Two of the Defendants in the SEC's civil case were also criminally charged for their conduct according to an indictment in the U.S. District Court for the District of New Jersey that was unsealed yesterday. The indictment in this case, U.S. v. Artem Radchenko and Oleksandr Ieremenko is available at: https://www.justice.gov/usao-nj/press-release/file/1124251/download.

[3] Of these Defendants, four are located in the Ukraine; four are in the Russian Federation; two are in Los Angeles; one is in Hong Kong; one is in Belize; and one is in the Republic of Korea. The "relief defendants" are individuals associated with non-relief Defendants whose accounts were used to effect trades on the information exfiltrated by the Hacker Defendant.

[4] More information about these newswire cases is available on the SEC's website at: https://www.sec.gov/news/pressrelease/2015-163.html; https://www.sec.gov/litigation/litreleases/2016/lr23471.htm; and https://www.sec.gov/litigation/litreleases/2018/lr24193.htm.

[5] Complaint at Paragraph 53.

[6] While these spoofed emails were sent to SEC computer users, FORTUNE magazine reported in March 2017 that cyber scammers were spoofing SEC emails. This article noted,

in part, that the cyber scammers were "sending spoofed emails, purporting to be from the SEC, and aiming them at lawyers, compliance managers, and other company officials who file documents with the SEC. . . . Those who clicked on instructions in the Word document granted the attackers access to internal corporate networks . . .."

According to the FORTUNE article, the security firm FireEye discovered these spoofed emails in February 2016 when it intercepted suspicious emails targeted at companies in sectors ranging from transportation to banking to retail. At the time, FireEye believed the scammers were likely an Eastern European criminal syndicate that was looking to make money by trading on inside information. *See "Fake SEC Emails Target Execs for Inside Information,"* Fortune (March 7, 2017), which is available at: http://fortune.com/2017/03/07/sec-phishing/.

[7] Complaint at Paragraph 68.

[8] Complaint at Paragraph 84.

[9] Complaint at Paragraph 144.
