October 28, 2019

Recent Cyber Attacks Target Asset Management Firms

A recent flurry of cyber attacks on asset managers should remind asset management firms and other financial institutions that they are attractive targets for cyber-exploitation and need to remain vigilant and institute appropriate preventative controls and monitoring procedures, as well as post-attack action plans.[1]

Many companies still see cyber attacks as one-off, anomalous events. But as recent events have shown, few are immune from illicit cyber-penetration and the frequency of these attacks continues to increase.

A recent spate of business email compromise schemes have involved fraudulent email messages sent to fund executives and officers.[2] The emails notify the recipients that they have an encrypted message, which they can access by clicking a link. Clicking the link causes malicious software to download onto the user's computer, gaining access to the user's account and perhaps further penetrating the institution's systems. While these and similar cyber schemes may sound like transparently suspicious and easy to detect attempts at blunt force penetration, their cost to businesses can be substantial, with some estimates exceeding $50 billion a year.[3] And considering the sheer volume of emails that asset management and other financial firms send and receive as a necessary part of conducting day-to-day business, even the most transparent cyber attacks are likely to succeed every once in a while.

Moreover, not all of the attacks are blunt force and transparent. Cybercriminals are employing increasingly sophisticated schemes and technologies. *The Wall Street Journal* recently reported on a cyber-fraud involving the use of artificial intelligence voice-impersonation software, which the perpetrators used to impersonate the voice of a company's CEO and call its subsidiary to arrange for a $243,000 wire transfer.[4] Given that phone verification is a common recommendation in the event of a suspicious-looking email, the

---

1 Leanna Orr, *Cyber Attack Hits Prominent Hedge Fund, Endowment, and Foundation*, INSTITUTIONAL INVESTOR, Oct. 24, 2019, https://www.institutionalinvestor.com/article/b1hqqxdl6pf03f/Cyber-Attack-Hits-Prominent-Hedge-Fund-Endowment-and-Foundation.

2 *Id.*

3 *See* The Council of Economic Advisors, *The Cost of Malicious Cyber Activity to the U.S. Economy*, Feb. 2018, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf; *Cyber Attacks Cost $45 Billion in 2018*, SECURITY MAGAZINE, Jul. 10, 2019, https://www.securitymagazine.com/articles/90493-cyber-attacks-cost-45-billion-in-2018; *see also* Federal Bureau of Investigation, Public Service Announcement (Sept. 10, 2019), https://www.ic3.gov/media/2019/190910.aspx#fn1 (reporting that business email compromise schemes alone were responsible for $26 billion in losses over a three-year period).

4 Catherine Stupp, *Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case*, WALL ST. J., Aug. 30, 2019, https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.

prospect of sophisticated voice impersonation emphasizes the need for more tailored procedures and controls.

Regulators recognize that financial firms are uniquely at risk, and have made cybersecurity a top priority, calling for companies to institute both prophylactic and remedial measures to deal with cyber attacks.[5] For example, the SEC Enforcement Division's Cyber Unit (formed in 2017) is tasked with investigating cybersecurity at regulated entities, as well as issuer disclosures of cybersecurity incidents and risks.[6] And, the SEC's Office of Compliance Inspections and Examinations (OCIE) continues to include cybersecurity among its Examination Priorities.[7]

This emphasis has been accompanied by an uptick in investigations and enforcement actions. In September, the CFTC reached a $1.5 million resolution (encompassing fines and restitution) with a futures commission merchant for failing to prevent, and then disclose, a successful phishing attack that resulted in a fraudulent $1 million withdrawal of customer funds.[8] The CFTC specifically alleged that the firm failed to comply with Regulations 166.3 and 1.55(i), which, under CFTC's interpretation, required mechanisms for the detection and deterrence of cybersecurity breaches and imposed an obligation (at least in certain circumstances) to disclose cybersecurity breaches.[9] Last September, the SEC settled an enforcement action against Voya Financial Advisors Inc. with a $1 million fine for Voya's alleged failure to protect confidential consumer information and prevent identity theft in connection with a 2016 cyber-intrusion. And last October, the SEC published a report on its investigation into public issuers that were victims of cyber-frauds resulting in losses of nearly $100 million, and whether the issuers were liable for failing to have sufficient internal accounting controls that could have prevented the losses.[10] The SEC ultimately decided not to pursue enforcement actions against those issuers, but its report sent a clear message that the SEC will not

---

5 Securities and Exchange Commission, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Release Nos. 33-10459, 34-82746 (Feb. 21, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf; *see* Paul, Weiss, *SEC Issues Updated Guidance on Cybersecurity Disclosure* (Feb. 27, 2018), https://www.paulweiss.com/media/3977641/27feb18-cybersecurity.pdf.

6 Securities and Exchange Commission, *Spotlight on Cybersecurity, the SEC and You*, https://www.sec.gov/spotlight/cybersecurity.

7 Securities and Exchange Commission, Office of Compliance Inspections and Examinations, *2019 Examination Priorities*, https://www.sec.gov/files/OCIE%202019%20Priorities.pdf.

8 U.S. Commodity Futures Trading Commission, *CFTC Orders Registrant to Pay $1.5 Million for Violations Related to Cyber Breach,* Release No. 8008-19 (Sept. 12, 2019), https://www.cftc.gov/PressRoom/PressReleases/8008-19, *see* Paul, Weiss, *CFTC Fines Phillip Capital for Failure to Prevent a Cyber Attack That Resulted in the Theft of Customer Funds* (Sept. 23, 2019), https://www.paulweiss.com/media/3978895/23sep19-cftc-phillip.pdf.

9 *In re Phillip Capital Inc.*, CFTC No. 19-22 (Sept. 12, 2019), https://www.cftc.gov/media/2476/enfphillipcapitalincorder091219/download.

10 Securities and Exchange Commission, *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*, Release No. 84429 (Oct. 16, 2018), https://www.sec.gov/litigation/investreport/34-84429.pdf.

treat financial firms as mere blameless victims of cybercrimes if they have not instituted robust preventative, monitoring, remedial, and disclosure mechanisms.[11]

What should asset management firms and other entities that have access to significant funds do? The answers are both simple and complex.

- No matter how robust your company's preventative access controls, monitoring procedures, and technical protections, some cyber attacks are bound to penetrate (even if they do not end up appropriating data or funds). But these controls are still an essential first line of defense for preventing and mitigating the vast majority of cyber attacks. And importantly, regulators expect to see them in place and continually updated.

- Companies also need to institute an action plan in the form of clear, thought-through policies and procedures to respond to cyber-penetrations if and when they occur. This should become part of a firm's general crisis management plans. Firms should contemplate lining up technical experts, executives, and counsel who can engage the necessary mitigation and disclosure procedures at an early stage. The right policies and procedures will not only ensure legal compliance, but perhaps even increase the chances of tracking down the location of the stolen funds and data and the perpetrators who took them.

* * *

[11] The SEC's broad focus on holding companies accountable when they are the victims of cybercrimes was also seen last April, when the SEC announced that Altaba, formerly known as Yahoo! Inc., agreed to pay a $35 million fine to settle charges that it misled investors by failing to disclose a data breach in which hackers stole personal data relating to hundreds of millions of Yahoo! accounts. *See* Paul, Weiss, *Yahoo! Agrees to $35 Million SEC Penalty for Failure to Disclose Cyber Incident* (May 3, 2018), https://www.paulweiss.com/media/3977759/3may18-yahoo.pdf.

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Roberto Finzi
+1-212-373-3311
rfinzi@paulweiss.com

Christopher D. Frey
+81-3-3597-6309
cfrey@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Udi Grofman
+1-212-373-3918
ugrofman@paulweiss.com

Jeh Charles Johnson
+1-212-373-3093
jjohnson@paulweiss.com

Lorin L. Reisner
+1-212-373-3250
lreisner@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Richard C. Tarlowe
+1-212-373-3035
rtarlowe@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

August Sangese
+1-212-373-3512
asangese@paulweiss.com

Associate Daniel J. Klein contributed to this Client Memorandum.