ALERTS

CFTC Cyber Incident Information Request — Private Fund Manager Responses Required

January 9, 2020

On Jan. 3, 2020, the National Futures Association distributed a Cyber Threat Alert from the U.S. Commodity Futures Trading Commission to registered commodity pool operators (i.e., many private fund managers) related to a cyber-intrusion affecting a number of cloud service providers, which was the focus of a Dec. 30, 2019 *Wall Street Journal* article.[1] The CFTC clarified the scope of its requests in a supplement sent on Jan. 9, 2020.

All registered private fund managers will have to take the following actions in response to the Cyber Threat Alert.

- *Directly Affected Managers*. CFTC-registered managers that engage cloud service providers impacted by the intrusion need to notify the CFTC's Division of Swap Dealer and Intermediary Oversight by Jan. 10, 2020, by emailing DSIOAlerts@CFTC.gov. Affected managers will need to include in their reply: (i) information regarding whether and when any provider informed them about the attack, (ii) a summary of any steps they have taken to protect their systems and data in response this attack and (iii) plans to notify market participants whose data may have been affected. Managers not affected by the attack need not reply to this request.

- *All CFTC-Registered Managers.* The Cyber Threat Alert asks that managers promptly notify the CFTC if their assessment of the impact of the intrusion changes.

- *All CFTC-Registered Managers*. The CFTC asked all managers "to consider, in light of this reporting, your organization's systems and data vulnerability." Managers therefore should address this CFTC request in their annual compliance reviews or, if that process is not imminent, in a separate review.

- *All Managers*. All Managers should consider what level of response to this situation is necessary or appropriate under their fiduciary obligations (understanding that regulators and investors may ask questions on this topic in the future).

The Cyber Threat Alert is a reminder that, to the extent managers experience *any* cyber intrusion, they should promptly review their disclosure obligations under their offering documents, regulatory filings, and investor agreements (including side letters), and consider any notification requirements under the rules of the NFA or any other applicable self-regulatory organization (the NFA has separate data breach notification requirements) and under state laws. These disclosures and responses will likely require the guidance of specialized privacy counsel.

Authored by Brian T. Daly, Edward H. Sadtler, Kelly Koscuiszka and Joshua B. Wright.

If you have any questions concerning this *Alert*, please contact your attorney at Schulte Roth & Zabel or one of the authors.

---

[1] The article reports that approximately a dozen cloud service providers have been hacked, and indicates that the attackers may have gained access to the providers' networks, compromising their clients' data in turn. *See* Rob Barry and Dustin Volz, "Ghosts in the Clouds: Inside China's Major Corporate Hack," *The Wall Street Journal*, Dec. 30, 2019, available here.

Related People

Kelly Koscuiszka

Partner

New York

Joshua Wright

Associate

New York

Practices

CYBERSECURITY AND DATA PRIVACY

INVESTMENT MANAGEMENT

REGULATORY AND COMPLIANCE

Attachments

Download Alert