The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 31801

June 11, 2019

SEC's OCIE Publishes a Risk Alert Relating to Registrants' Use of Third-Party Electronic Storage Solutions

[31801]

June 11, 2019 TO: ICI Members
Investment Company Directors
Chief Compliance Officer Committee
Chief Information Security Officer Advisory Committee
Chief Risk Officer Committee
Internal Audit Committee
Operations Committee
Technology Committee
Transfer Agent Advisory Committee SUBJECTS: Cybersecurity
Systemic Risk RE: SEC's OCIE Publishes a Risk Alert Relating to Registrants' Use of Third-Party Electronic Storage Solutions

The SEC's Office of Compliance Inspections and Examinations (OCIE) recently published a Risk Alert related to the use of third-party network storage solutions, such as cloud storage services. This 2-page Risk Alert, *Safeguarding Customer Records and Information In Network Storage – Use of Third Party Security Features,*[1]discusses those practices that OCIE has observed relating to this topic that may raise compliance concerns under Regulations S-P and S-ID.[2] It is intended to highlight the risk associated with storing records in the cloud or on other types of third-party network storage solutions. As noted in the Risk Alert, "[a]lthough the majority of these network storage solutions offered encryption, password protection, and other security features designed to prevent unauthorized access, examiners observed that firms did not always use the available security features." As a result, the stored data may be subject to unauthorized access.

Examples of Security Weaknesses

The three concerns highlighted by OCIE in the Risk Alert are:

1. **Misconfigured network storage solutions.** According to OCIE, while some firms did not adequately configure the security settings on their network storage solutions to protect against unauthorized access of the data, others did not have policies and procedures addressing this issue. As noted by OCIE, "[o]ften, misconfigured settings resulted from a lack of effective oversight when the storage solution was initially

implemented."

2. **Inadequate oversight of vendor-provided network storage solutions.** OCIE observed some firms failing to ensure, through policies, procedures, contractual provisions, or otherwise, that the security settings on the network storage solutions were configured in accordance with the firm's standards.
3. **Insufficient data classification policies and procedures.** The final area of concern observed by OCIE involved firms' policies and procedures failing to identify the different types of data stored electronically by the firm and the appropriate level of security controls for each type of data.

Examples of Effective Practices

In addition to highlighting the above areas of concern, the Risk Alert also includes examples of effective practices observed by OCIE, which are as follows:

- Policies and procedures designed to support the initial installation, on-going maintenance, and regular review of the network storage solution;
- Guidelines for security controls and baseline security configuration standards to ensure that each network solution is properly configured; and
- Policies and procedures relating to vendor management that include, among other things, regular implementation of software patches and hardware updates, followed by reviews to ensure that such patches or updates "did not unintentionally change, weaken, or otherwise modify the security configuration."

OCIE published the Risk Alert, in part, to encourage firms to both (1) review their current practices in this area to see if any improvements are necessary and (2) actively oversee their network storage vendors to ensure that the firm is meeting its regulatory requirements under Regulations S-P and S-ID.

Tamara K. Salmon
Associate General Counsel

endnotes

[1] The Risk Alert is *available at* https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf.

[2] As noted in footnote 2 to the Risk Alert:

> The Safeguards Rule of Regulation S-P requires every broker-dealer and investment adviser registered with the Commission to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. 17 C.F.R. 248.30(a). The Identity Theft Red Flags Rule of Regulation S-ID requires broker-dealers and investment advisers registered or required to be registered with the Commission to develop and implement a written identity theft prevention program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. 17 C.F.R. 248.201. A covered account includes an account that a broker-dealer or investment adviser offers or maintains, primarily for personal, family, or

household purposes, that involves or is designed to permit multiple payments or transactions. 17 C.F.R. 201(b)(3).
