The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 31725

April 23, 2019

OCIE Publishes Risk Alert Listing Compliance Issues Related to Regulation S-P Found During Exams Over the Past Two Years

[31725]

April 23, 2019 TO: ICI Members
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: Compliance
Cybersecurity RE: OCIE Publishes Risk Alert Listing Compliance Issues Related to Regulation S-P Found During Exams Over the Past Two Years

As you likely know, the SEC's Office of Compliance Inspections and Examinations (OCIE) is currently conducting its third round of inspections focused on registrants' cybersecurity efforts. During these inspections, among other things, OCIE will be reviewing registrants' policies and procedures implementing Rule 248.30 of Regulation S-P, which is referred to as the "Safeguards Rule."[1] As OCIE continues with these inspections, last week it published a Risk Alert that highlights "the most common deficiencies or weaknesses identified by OCIE staff in connection with the Safeguards Rule" that were "identified in deficiency letters from broker-dealer and adviser exams completed during the past two years."[2]

Most of the deficiencies and weaknesses highlighted in the Risk Alert relate to registrants either not designing adequate policies and procedures to implement the Rule's requirements to safeguard customer records and information or not implementing their written policies and procedures under the Rule.[3] The deficiencies and weaknesses listed in the Risk Alert involved the following areas:

- **Personal Devices.** OCIE staff observed registrants failing to have policies and procedures governing the security of customers' information maintained or stored on employees' laptops.
- **Electronic Communications.** According to OCIE, some registrants failed to have

policies and procedures reasonably designed to prevent employees from regularly sending unencrypted emails to customers when such emails contained personally identifiable information.

- **Training and Monitoring.** The staff observed registrants either failing to provide employees adequate training on the registrant's policies and procedures under the Safeguards Rule or failing to monitor that such policies were being followed by employees.
- **Unsecure Networks.** The staff observed policies and procedures that did not prohibit employees from sending customers' personal information to unsecure locations outside the firm's networks.
- **Outside Vendors.** With respect to outside vendors, OCIE noted that some registrants failed to require vendors to maintain the confidentiality of customer information even though the registrant's policies required it to have such contractual provisions.
- **PII Inventory.** According to OCIE, some registrants' policies and procedures failed to identify all systems on which the registrant maintained customers' personally identifiable information. As noted in the Risk Alert, the absence of such an inventory could limit the registrant's ability to adopt reasonably designed policies and procedures and adequately safeguard such information.
- **Incident Response Plan.** The staff found instances in which the registrant's written response plan in the event of an incident or breach failed to address issues such as role assignments for implementing the plan, actions to take in the event of a cyber incident, and assessment of system vulnerabilities.
- **Unsecure Physical Locations.** The staff observed customer information being stored in unsecured physical locations such as in unlocked file cabinets in open offices.
- **Login Credentials.** According to OCIE, it observed customer login credentials that were disseminated to more employees than permitted by the firms' policies and procedures.
- **Departed Employees.** The staff observed instances where because former employees of the registrant retained access rights after their departure, they would be able to access restricted customer information.

As OCIE continues to focus on cyber issues, and as it conducts its third round of cyber reviews, members should expect that OCIE will be reviewing the above areas, among others, as part of these reviews. According to OCIE's webpage, the "key takeaway" from the Risk Alert is that "registrants should review their written policies and procedures, including implementation of those policies and procedures, to ensure that they are in compliance with the relevant regulatory requirements."[4]

The Risk Alert also references the Risk Alert OCIE published in August 2017 that discussed observations from OCIE's second round of cybersecurity reviews, which involved 75 registrants.[5] Unlike the current Risk Alert, the August 2017 Risk Alert included a list of "elements of robust policies and procedures" OCIE observed as part of their reviews.[6] As OCIE continues to focus on cyber issues, and as it conducts its third round of cyber reviews, registrants should expect that OCIE will be reviewing, among others, the above areas and those discussed in the 2017 Risk Alert as part of these reviews.

Tamara K. Salmon
Associate General Counsel

endnotes

[1] Rule 248.30 of Regulation S-P requires registrants to have "written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." Such policies and procedures must: insure the security and confidentiality of such records; protect them from anticipated threats to their integrity; and protect them against unauthorized access. This is the provision the SEC cites in enforcement proceedings when a registrant experiences a breach that impacts customers' non-public personal information.

[2] *See Risk Alert: Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies,* OCIE (April 16, 2019), which is available at: https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf.

[3] The Risk Alert also discusses registrants' failure to comply with provisions in Regulation S-P that require them to: (1) provide initial or annual privacy notices or opt-out notices to their customers; (2) provide customers accurate privacy notices; and (3) have written policies and procedures implementing the Safeguards Rule.

[4] *See* https://www.sec.gov/ocie/announcement/ocie-risk-alert-regulation-s-p.

[5] *See Risk Alert: Observations from Cybersecurity Examinations,* OCIE (August 7, 2017), which is available at: https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf. *See, also,* ICI Memorandum No.30830 (August 11, 2017), which summarized this Risk Alert.

[6] This list includes: maintenance of an inventory of data, information, and vendors; detailed cybersecurity-related instructions; maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities; established and enforced controls to access data and systems; mandatory employee training; and engaged senior management. Each of these areas were discussed in more detail in the Risk Alert.
