PUBLICATIONS

OCIE Focusing on Safeguarding of Customer Information and Books and Records Retention

SRZ Private Funds Regulatory Update

August 2019

The SEC's Office of Compliance Inspections and Examinations ("OCIE") has recently issued risk alerts relating to the safeguarding of customer information and books and records retention obligations. OCIE has issued three risk alerts relating to (i) the Safeguards Rule of Regulation S-P, (ii) the security risks associated with cloud storage providers and (iii) books and records retention obligations related to the use of electronic messaging. In addition, the SEC's staff ("Staff") has recently sent inquiries to many advisers requesting information on their use of cloud storage providers.[1]

1. *Risk Alert on Safeguards Rule of Regulation S-P.* In a Risk Alert issued on April 16, 2019, OCIE identified common deficiencies under Regulation S-P,[2] including advisers failing to implement policies and procedures reasonably designed to comply with Regulation S-P, as well as deficiencies in implementation, such as a lack of relevant training and monitoring, unsecure networks, and unimplemented or insufficiently tailored policies governing the use of personal electronic devices and outside data vendors. To the extent that investor records and information are maintained in databases administered by cloud storage providers, the requirements of the Safeguard Rule could apply to the use of such vendors.

2. *Risk Alert on Security of Cloud Storage Providers*. On May 23, 2019, OCIE published an additional Risk Alert focusing on the security risks associated with storage of customer data by investment advisers, including through cloud-based solutions. OCIE highlighted potential deficiencies that implicate data protection and oversight issues under Regulations S-P and S-ID (Identity Theft Red Flags rule), including:

- Misconfigured network storage solutions (which are incapable of ensuring only authorized access) and the lack of policies addressing the security configuration of network storage;
- Inadequate oversight of vendor-provided network storage solutions, such as through a failure to adopt policies, procedures, contractual provisions, or otherwise, that ensure the security settings on vendor-provided network storage solutions were configured in accordance with the firm's standards;
- Insufficient data classification policies and procedures, such as through a failure to identify the types of data stored by a firm and appropriate controls for each type of data.

In the Risk Alert, OCIE noted a configuration management program that includes policies and procedures governing data classification, vendor oversight and security features will help to mitigate the risks incurred when implementing on-premises or cloud-based network storage solutions. OCIE identified several features of effective configuration management programs, data classification procedures and vendor management programs, based on examination findings.

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

3. *Risk Alert on Retention of Electronic Messaging Records*. OCIE's focus on the use of cloud storage providers is another instance of its recent focus on records retention. OCIE raised similar issues in a December 2018 Risk Alert addressing the use of electronic messaging for business practices, where it identified practices that could be helpful to advisers in complying with related books and records retention obligations. The practices identified in this Risk Alert were based on the Staff's observations from a recent examination sweep focused on the use of text/SMS messaging, instant messaging, personal email and personal or private messaging ("Electronic Messaging") by advisers and their personnel to conduct business-related communications. OCIE's sweep specifically excluded the use of firm email accounts.

In the Risk Alert, OCIE identified four recommended policies or procedures that advisers should adopt to enhance oversight and review of employee activity in the use of Electronic Messaging:

- For advisers who allow the use of social media, personal email or personal websites, engaging third-party vendors to monitor the use of those platforms, archive their use for compliance with the SEC's Books and Record Rule and review content for key words and phrases to identify changes in content or flag other issues;
- Reviewing social media sites on a regular basis to determine whether advisory personnel are using social media to conduct firm business, particularly to detect circumvention of complete or partial prohibitions on the use of social media for business purposes;
- Conducting regular searches, or setting up automated alerts of advisory personnel on various websites to determine whether unauthorized firm business is being conducted online; and
- Arranging an anonymous or confidential system through which employees can report any Electronic Messaging, social media posting or website communications which may be considered conducting firm business through an unapproved platform.

OCIE further identified certain cybersecurity practices which may enhance advisers' insight into and control over advisory personnel use of Electronic Messaging for business purposes, including (i) requiring employees to obtain pre-approval for the use of firm applications, including Electronic Messaging apps, on personal devices; (ii) loading

security software on firm-issued or personal devices that roll out cybersecurity updates, monitor for prohibited applications and delete locally stored information from devices that have been reported as lost or stolen; and (iii) only allowing access to advisers' email servers through VPN, or other similar secure connection.

In light of OCIE's recent risk alerts and inquires, advisers should review their practices, policies and procedures with respect to the storage of electronic customer information, the use of cloud storage providers and the retention of records created by the use of Electronic Messaging. Advisers should consider whether their policies and procedures address the areas identified by the Staff with respect to recordkeeping, training, due diligence and cybersecurity.

This article appeared in the August 2019 edition of the *SRZ Private Funds Regulatory Update*. To read the full *Update*, click here.

---

[1] Advisers commonly utilize cloud storage providers for books and records retention, and the staff of the SEC's Division of Investment Management first addressed the use of such services in the *Omgeo LLC* no-action letter (August 14, 2009), stating that it would not recommend enforcement against an adviser utilizing cloud storage providers for records retention, provided that the adviser can access those records from its principal place of business.

[2] The Safeguards Rule of Regulation S-P (which is itself the main SEC rule governing privacy notices and procedures for investment advisers) requires every investment adviser registered with the SEC 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) (2004).

Related People

Marc Elovitz

Partner

New York

Anna Maleva-Otto

Partner

London

Practices

REGULATORY AND COMPLIANCE

INVESTMENT MANAGEMENT

CYBERSECURITY AND DATA PRIVACY

Attachments

Read Article

Read Update