Proskauer

OCIE Releases Risk Alert for Investment Advisers and Broker-Dealers, Under Regulation S-P

April 25, 2019

On April 16, 2019, the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued a Risk Alert, based on compliance issues identified in recent examinations of investment advisers registered with the SEC and brokers and dealers ("registrants") relating to Regulation S-P, the primary SEC rule regarding privacy notices and safeguarding policies of registrants. This Risk Alert builds upon an SEC-published reference guide, Questions Advisers Should Ask While Establishing or Reviewing Their Compliance Programs, as well as prior OCIE-published Risk Alerts. This most recent Risk Alert highlights common deficiencies and weaknesses with registrants' privacy policies and procedures, both in form and in implementation.

Deficiencies in Policies and Procedures

Regulation S-P requires that all registrants adopt written policies and procedures that are reasonably designed to (a) ensure the security and confidentiality of consumer records and information, (b) protect against any anticipated threats or hazards to the security or integrity of customer records and information, and (c) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

OCIE found that registrants either did not have written policies and procedures that complied with this rule, or had policies and procedures that reiterated the rule but did not actually incorporate administrative, technical, or physical safeguards into the policies and procedures. OCIE noted deficiencies with respect to:

- Personal devices, which regularly were used to store and maintain customer information, despite a lack of clarity in policies and procedures around how the devices should be configured to protect this information;
- Electronic communications of personally identifiable information, as policies and procedures, for example, were not designed to prevent employees from sending

unencrypted emails containing the information;

- Training and monitoring of employees, to instill the practice of encrypting and password protecting consumer information and using only registrant-approved methods to transmit customer information;
- Unsecure networks, as policies and procedures did not prevent employees from sending personally identifiable information to unsecured networks;
- Outside vendors, which were not required to comply with the requirements in registrants' formal policies and procedures;
- Inventories of personally identifiable information, which were not maintained, leaving registrants potentially unaware and unable to safeguard the categories of information maintained;
- Incident response plans, which did not address key areas such as role assignments, response to a cybersecurity incident, and system vulnerability assessments;
- Unsecure physical locations, such as open offices and unlocked file cabinets, where customer personally identifiable information was stored;
- Customer login credentials, which had been shared with more employees than allowed under relevant policies and procedures; and
- Departed employees, who retained access rights to restricted customer information post-departure.

Deficiencies in Privacy and Opt-Out Notices

Regulation S-P further requires that registrants provide clear and conspicuous notice to customers, which accurately reflects its privacy policies and practices, during (a) the initial establishment of a customer relationship and (b) not less than annually during the customer relationship. This clear and conspicuous notice must explain the right to opt out of certain disclosures of nonpublic personal information about the customer to third parties unaffiliated with the registrant.

OCIE observed that registrants failed to provide these required notices to customers. When notices were provided, they did not necessarily accurately reflect the firms' policies and procedures. They also did not include the right to opt out of sharing nonpublic personal information with third parties.

Conclusion

This Risk Alert provides guidance for investment advisers and broker-dealers to review their written policies and procedures to ensure that they are compliant both in form and in practice. Please feel free to contact us with any questions.