Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

SEC Warns Registered Firms about Client Privacy and Data Security

April 26, 2019

Key Points

- The SEC released a Risk Alert summarizing key areas in which it continues to see compliance deficiencies related to Regulation S-P, the primary SEC rule regarding privacy notices and safeguard policies of investment advisors and broker-dealers.
- Registered firms should review their written policies and procedures and implementation of the same to ensure compliance with Reg S-P and guidance in the latest alert.
- Firms should: (1) provide customers with initial and annual privacy notices, and opt-out notices that reflect the firm's policies and procedures; (2) establish written policies and procedures related to administrative, technical, and physical safeguards; and (3) implement and reasonably design policies to safeguard customer records and information.

1. Introduction

On April 16, 2019, the Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert warning investment advisors and broker-dealers to review their policies and procedures regarding Regulation S-P ("Reg S-P"), a privacy rule designed to safeguard customer records and information that is also known as the Safeguards Rule and the Identity Theft Red Flags Rule. (See full Risk Alert here.) OCIE issued the alert after seeing repeated deficiencies in Reg S-P compliance during examinations.

The SEC's latest Risk Alert comes on the heels of a recently announced enforcement action regarding Reg S-P, which resulted in a $1 million fine for failed policies and procedures that resulted in a breach. (SEC Press Release.) The SEC's recent Risk Alert continues the recent emphasis on Reg S-P and cybersecurity and data privacy generally. The SEC details two key requirements of Reg S-P: privacy and opt-out notices and written policies and procedures.

- Privacy and Opt-Out Notices: Reg S-P requires a firm to provide a "clear and conspicuous notice" to customers that accurately reflects the firm's privacy policies and practices upon establishing a customer relationship ("Initial Privacy Notice") (17

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Peter I. Altman
Partner
paltman@akingump.com
Los Angeles
+1 310.728.3085

Diana E. Schaffner
Counsel
dschaffner@akingump.com
San Francisco
+1 415.765.9507

Nicole Ashley Greenstein
Associate
ngreenstein@akingump.com
New York
+1 212.872.1068

CFR § 248.4), as well as not less than annually throughout the customer relationship ("Annual Privacy Notice") (17 CFR § 248.5). It also requires a firm to deliver a "clear and conspicuous notice" to customers that accurately explains the right to opt out of some disclosures of the customer's non-public personal information to third parties ("Opt-Out Notice") (17 CFR § 248.7). Reg S-P provides clear guidance on what should be included in these notices. Use of the SEC's model notice form provides a "safe harbor" from claims related the privacy notice (17 CFR § 248.2).

- Written Policies and Procedures to Safeguard Customer Information: Reg S-P's Safeguard Rule requires firms to adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information (17 CFR 248.30(a)). Policies and procedures must be reasonably designed to ensure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of customer records and information, and protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

2. Common Compliance Issues

OCIE listed the most common deficiencies regarding Reg S-P that its staff discovered during examinations. These deficiencies fell into three categories: (1) privacy and opt-out notices, (2) a lack of policies and procedures and (3) policies that were not implemented or not reasonably designed to safeguard customer records and information.

A. Privacy and Opt-Out Notices

OCIE staff observed firms that did not provide Initial Privacy Notices, Annual Privacy Notices and Opt-Out Notices to their customers. Some firms provided notices that did not accurately reflect the firm's policies and procedures.

Firms should ensure that they are regularly providing customers with all privacy notices and opt-out notices required by Reg S-P and that these notices accurately reflect the firm's policies and procedures.

B. Lack of Policies and Procedures

OCIE staff also discovered some firms still do not have written policies and procedures as required by the Safeguards Rule. Some firms simply restated the Safeguards Rule, without including policies and procedures related to administrative, technical and physical safeguards. A firm's policies and procedures must do more than simply address the delivery and content of a Privacy Notice to comply with the Safeguards Rule. OCIE also found firms with written policies and procedures that "contained numerous blank spaces designed to be filled in by registrants."

Firms should ensure that they have comprehensive policies and procedures in place that address administrative, technical and physical safeguards, as required by Reg S-P. These policies and procedures should be specifically tailored to the firm, rather than generic, boilerplate provisions.

C. Policies Not Implemented or Not Reasonably Designed to Safeguard Customer Records and Information

OCIE staff observed firms with written policies and procedures that did not comply with the Safeguard Rule inasmuch as they either were not implemented or were not reasonably designed to: (1) ensure the security and confidentiality of customer records and information; (2) protect against anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to customers.

To comply with the Safeguard Rule, a firm's policies and procedures should be comprehensive. The following are a few key areas that the OCIE highlighted in the recent alert that should be covered in a firm's policies and procedures.

- Outside Vendors: Adopt and implement strong policies and procedures concerning outside vendors that require vendors to meet certain security benchmarks. Monitor your vendors to ensure they comply with their contractual obligations.
- PII Inventory: Inventory all systems on which the firm maintains customer personally identifiable information (PII). Ensure policies and procedures account for the results of this inventory.
- Incident Response Plans: Adopt, implement and test written incident response plans that provide real-life guidance to facilitate quick plan implementation and that take into account known system vulnerabilities.
- Personal Devices: Adopt and implement policies and procedures to safeguard customer information on personal devices (personal laptops, smartphones, iPads, etc.) and explain the same to employees.
- Training and Monitoring: Train employees on encryption, password protection and other security measures. Regularly test employees through routine fake phishing exercises and similar activities to ensure compliance.

Conclusion

The OCIE alert serves as a warning to firms to avoid the same mistakes that others have repeatedly made over the last two years. SEC-registered firms should carefully review their written policies and procedures, as well as how these policies are procedures are implemented, to ensure full compliance with Reg S-P. At a minimum, firms should ensure that: (1) they provide customers with initial and annual privacy notices, as well as opt-out notices, that actually reflect their policies and procedures; (2) they have written policies and procedures related to administrative, technical and physical safeguards; and (3) their policies are implemented and reasonably designed to safeguard customer records and information.

Our team will continue to monitor the latest developments regarding the Reg S-P, as well as the SEC's continued focus on cybersecurity risk and compliance.

akingump.com