WILMERHALE

OCIE Issues Risk Alert Regarding Advisers and Broker-Dealers Failing to Comply with Regulation S-P

MAY 15, 2019

On April 16, 2019, the Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) released a new Risk Alert[1] regarding Regulation S-P deficiencies found in recent examinations of SEC-registered investment advisers and broker-dealers.[2] Regulation S-P is the SEC's primary rule regarding privacy notices and safeguard policies of SEC-registered investment advisers and broker-dealers (each, a "firm").

Regulation S-P at a Glance

Among other things, Regulation S-P requires that a firm provide (1) a clear and conspicuous notice to its customers[3] that accurately reflects its privacy policies and practices when it initially establishes a customer relationship and at least annually during such relationship ("Privacy Notices") and (2) a clear and conspicuous notice to its customers explaining that they have the right to opt out of the firm disclosing the customer's nonpublic personal information to nonaffiliated third parties in some instances ("Opt-Out Notice").

Further, one of the rules under Regulation S-P requires firms to adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information (the "Safeguards Rule"). Pursuant to the Safeguards Rule, such written policies and procedures must be 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 any customer.[4]

OCIE's Findings

While the Risk Alert does not address all the weaknesses the OCIE staff identified, it sets forth the most frequent deficiencies found by the staff in connection with the Safeguards Rule:

- *Privacy and Opt-Out Notices*. Firms failed to provide Privacy or Opt-Out Notices to their customers or provided notices that either did not accurately reflect their policies and procedures or did not inform customers of their opt-out right.

- *Lack of Policies and Procedures*. Firms failed to adopt the requisite written policies and procedures under the Safeguards Rule (e.g., firms had documents that simply restated the Safeguards Rule but did not include specific policies and procedures related to administrative, technical and physical safeguards of customer records and information). Further, certain written policies and procedures reviewed by OCIE's staff contained numerous blank spaces meant to be completed by the firms.
- *Implementation and Design of Policies and Procedures*. Firms maintained written policies and procedures that were not implemented or reasonably designed to safeguard customer records and information as set forth by the Safeguards Rule. For instance, OCIE staff observed:
  - Personal Devices. Policies and procedures that were not reasonably designed to safeguard customer information on personal devices (e.g., proper configuration of firm employees' personal laptops that stored customer information).
  - Electronic Communications. Policies and procedures that did not address the inclusion of customer personally identifiable information (PII) in electronic communications (e.g., some firms did not appear to have policies and procedures reasonably designed to prevent employees from regularly sending unencrypted emails containing PII to customers).
  - Training and Monitoring. Policies and procedures that, although they required customer information to be encrypted, password-protected and transmitted using only firm-approved methods, were not reasonably designed because *employees were not provided adequate training* on these methods and the firm *failed to monitor* whether the policies were being followed by employees.
  - Unsecured Networks. Policies and procedures that failed to prohibit employees from sending customer PII to unsecure locations outside of the firm's network.
  - Outside Vendors. Failures by firms to follow their own policies and procedures with respect to outside vendors (e.g., firms failed to require outside vendors to contractually agree to keep customers' PII confidential despite having such requirement in their policies and procedures).
  - PII Inventory. Failures by firms to institute policies and procedures that identify all systems on which the firm stored customer PII.
  - Incident Response Plans. Failures of firms' written incident response plans to address important areas (e.g., actions required to address a cybersecurity incident, role assignments for implementing the plan or assessments of system vulnerabilities).
  - Unsecured Physical Locations. Storing by firms of customer PII in unsecure physical locations (e.g., in unlocked file cabinets in open offices).
  - Departed Employees. Retention by some firms' former employees of access rights to firm systems following their departure, which could provide for access to restricted customer information.
  - Login Credentials. Customer login credentials that had been shared with more employees than permitted under firms' policies and procedures.

Takeaways

While most investment advisers and broker-dealers have policies and procedures in place relating to Regulation S-P, many of these seem to be inadequate and/or inadequately communicated to employees. OCIE's Risk Alert focuses on ensuring compliance with each aspect of Regulation S-P as well as compliance with a firm's policies and procedures. Thus, firms should review their policies and procedures, as well as their actual practices and documentation, for compliance with Regulation S-P, particularly the Safeguards Rule. Firms should also enhance their training and monitoring of these policies as they require all employees to understand and comply. The laundry list of deficiencies and weaknesses noted in the Risk Alert is a good road map to help work through a firm's potential weaknesses, leading to a more comprehensive review.

---

1. The official release.

2. 17 CFR Part 248, Subpart A, and Appendix A to Subpart A.

3. Under Regulation S-P, a "customer" is a consumer who has a continuing relationship with a firm under which the firm provides one or more financial products or services to the consumer. For instance, an individual with whom an investment adviser has an investment advisory contract (whether written or oral) would be a customer of the adviser. Similarly, "customer" includes an individual that has a brokerage account with a broker-dealer.

4. 2004 amendments to Regulation S-P clarify that persons under the purview of the rule that dispose of "consumer report information" must take reasonable measures to protect the discarded information from unauthorized access to or use of it (e.g., shredding, burning or pulverizing of paper records). *See Inv. Adv. Act. Rel. No. 2332*, 2004 SEC Lexis 2823 (Dec. 2, 2004).

Authors

Timothy F. Silva

PARTNER

Chair, Investment Management Practice

timothy.silva@wilmerhale.com

+1 617 526 6502

Wilmer Cutler Pickering Hale and Dorr LLP is a Delaware limited liability partnership. WilmerHale principal law offices: 60 State Street, Boston, Massachusetts 02109, +1 617 526 6000; 2100 Pennsylvania Avenue, NW, Washington, DC 20037, +1 202 663 6000. Our United Kingdom office is operated under a separate Delaware limited liability partnership of solicitors and registered foreign lawyers authorized and regulated by the Solicitors Regulation Authority (SRA No. 287488). Our professional rules can be found at www.sra.org.uk/solicitors/code-of-conduct.page. A list of partners and their professional qualifications is available for inspection at our UK office. In Beijing, we are registered to operate as a Foreign Law Firm Representative Office. This material is for general informational purposes only and does not represent our advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised of all legal developments. Prior results do not guarantee a similar outcome. © 2004-2024 Wilmer Cutler Pickering Hale and Dorr LLP