Published on *The National Law Review* https://natlawreview.com

On Cybersecurity, Grab the Low-Hanging Fruit

Article By:

Michael L. Yaeger

SEC Tells Firms to Stop Missing the Basics on Cybersecurity

The SEC's Office of Compliance Inspections and Examinations (OCIE) reported in a recent Risk Alert that many investment advisers and broker-dealers are failing to comply with basic aspects of Regulation S-P, which requires registered firms to **provide customers with privacy notices** and to **safeguard customers' records and information**. The observed deficiencies are especially notable as they are basic flaws already discussed in previous SEC guidance; failure to correct them may lead to fines or even significant consequences in private suits by investors. Faced with such deficiencies, a court might conclude that a firm has not taken reasonable measures to safeguard customer information.

Regulation S-P requires that firms provide customers with initial notices regarding their privacy policies and practices when they sign up, with annual notices throughout the customer relationship, and with "opt-out" notices describing customers' right to forbid disclosure of nonpublic personal information to nonaffiliated third parties. But OCIE observed in recent examinations that many firms did not provide such notices, and that when they did, the notices did not always accurately reflect firms' policies and procedures.

OCIE also noted that firms failed to implement a host of basic policies and procedures designed to ensure the confidentiality and integrity of customer information. Deficiencies included:

- lack of policies and procedures to prevent employees from regularly sending unencrypted emails containing personally identifiable information (PII);
- lack of training on the use of encryption;
- failure to create an inventory identifying all systems on which the firm maintained customer PII;
- failure to revoke the system access rights of departed employees;
- contracts with outside vendors where the vendors did not agree to keep customers' PII confidential, even though such agreement was mandated by the firm's policies and procedures; and

- incident response plans that omitted “role assignments for implementing the plan, actions required to address a cybersecurity incident, and assessments of system vulnerabilities.”

Especially because the SEC staff has now provided multiple warnings, such deficiencies deserve more attention.

National Law Review, Volume IX, Number 203