LEGALcurrents®

May 3, 2019

Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

SECURITIES AND CAPITAL MARKETS

PRIVACY AND DATA SECURITY

SEC IDENTIFIES CYBERSECURITY COMPLIANCE ISSUES FOLLOWING EXAMINATIONS

Author: Laura K. Schwalbe

On April 16, 2019, the Securities and Exchange Commission ("SEC") Office of Compliance Inspections and Examinations ("OCIE") issued a Risk Alert following OCIE's examinations of investment advisers and broker-dealers. The Risk Alert identified some of the key compliance issues in the recent examinations related to Regulation S-P, which is the SEC's principle rule covering privacy notices and policies and practices required to safeguard customer records and information.

Regulatory Requirements

Regulation S-P requires investment advisers and broker-dealers to provide a number of notices regarding privacy policies and practices. An initial notice detailing policies and practices must be sent by the time a customer relationship exists and investment advisers and broker-dealers must continue to send notices at least once annually for as long as the customer relationship exists. Additionally, investment advisers and broker-dealers must send an opt-out notice to customers that explains a customer's right to opt-out of some disclosures of non-public personal information that the investment advisers and broker-dealers might otherwise make to nonaffiliated third parties.

The SEC also requires investment advisers and broker-dealers to adopt written policies and procedures covering administrative, technical, and physical safeguards for the protection of customer records and information. Regulation S-P requires that these policies and procedures be reasonably designed to (1) protect the security and confidentiality of records and information; (2) protect against anticipated threats or hazards to the security or integrity of records and information; and (3) protect against unauthorized access to or use of records or information that could result in harm or inconvenience to a customer.

Key Issues Uncovered During OCIE Examinations

The Risk Alert detailed a number of common deficiencies or weaknesses observed by OCIE staff in their examinations of investment advisers and broker-dealers.

In connection with privacy notices, OCIE staff found numerous situations where the required notices (initial, annual, and opt-out) were not sent at all. The staff also found that even when notices were sent, they did not always accurately reflect current policies and practices or advise customers of their right to opt-out of some disclosures to nonaffiliated third parties.

OCIE staff also noted numerous situations where investment advisers and broker-dealers did not have written policies and procedures that complied with the Regulation S-P requirements. Even where an investment adviser or broker-dealer had policies or procedures, OCIE staff noted numerous areas where it observed either deficiencies in the content of the policies or procedures or weaknesses in the implementation of the policies or procedures. Some of the more common observations included:

- Employees who stored customer information on personal laptops without a company policy that addressed how such usage should be configured to safeguard such information.
- Lack of policies or procedures covering how electronic communications containing customers' personally identifiable information ("PII") should and should not be sent.
- Failing to train employees on policies and procedures or monitor whether policies were being followed.
- Failing to ensure that policies and procedures regarding outside vendors were followed.
- Lack of an accurate inventory of all systems that contain customer PII.
- Deficient incident response plans that failed to address areas such as role assignments, responses to a cybersecurity incident, or assessments of system vulnerabilities.
- Storage of PII in unsecure locations, such as unlocked file cabinets in open offices.
- Improper access to customer information, including situations where information was shared to more employees than permitted under policies and procedures, or situations where former employees retained access to restricted information after departure.

Conclusion

Protection of sensitive customer records and information is, and will almost certainly remain, one of the biggest challenges facing all types of companies. The compliance issues discussed in this SEC Risk Alert will continue to be a focus of the SEC in examinations and investigations. It is incumbent upon companies to engage in a thorough review of the existence, implementation, and operation of practices, procedures, and policies to ensure compliance with regulatory requirements.

If you would like more information regarding compliance with SEC rules relating to cybersecurity or best practices for preparing for and avoiding a cybersecurity incident, please contact a member of Harter Secrest & Emery LLP's Securities and Capital Markets Group or Privacy and Data Security Group. For more information, visit www.hselaw.com.

Laura K. Schwalbe, 716.844.3752, lschwalbe@hselaw.com