THE
NATIONAL LAW REVIEW

SEC Issues Privacy and Data Security Risk Alert

Thursday, April 18, 2019

Article By Jackson Lewis P.C.
Joseph J. Lazzarotti
Workplace Privacy Blog

Securities & SEC
All Federal

Following recent examinations of SEC-registered investment advisers and broker-dealers, the Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) published a privacy risk alert on April 16, 2019. OCIE is hoping to remind advisers and broker-dealers about providing compliant privacy and opt-out notices, and adopting and implementing effective policies and procedures for safeguarding customer records and information, under Regulation S-P.

Privacy Notices. During the examinations, OCIE observed advisors and broker-dealers were not providing initial privacy notices, annual privacy notices and opt-out notices to their customers. When these notices were provided, many did not accurately reflect firms' policies and procedures and/or notify customers of their right to opt out of having their nonpublic personal information shared with nonaffiliated third parties. OCIE's risk alert, thus, reminds advisors and broker-dealers that Regulation S-P requires that they:

- provide a clear and conspicuous notice to customers that accurately reflects privacy policies and practices generally no later than when a customer relationship is established,
- provide a similar notice not less than annually during the continuation of the customer relationship, and
- deliver a clear and conspicuous notice to its customers that accurately explains the right to opt out of some disclosures of non-public personal information about the customer to nonaffiliated third parties.

Written Policies and Procedures to Safeguard Customer Information. OCIE also observed during these examinations that some advisors and broker-dealers had not adopted written policies and procedures as required under the Safeguards Rule. According to the risk alert, some firms simply:

> ***restated the Safeguards Rule but did not include policies and procedures related to administrative, technical, and physical safeguards.***

And, other policies

> ***contained numerous blank spaces designed to be filled in by registrants.***

Given the OCIE's observations, purchasing sample privacy and data and security policies and procedures, perhaps online, without more, would likely be inconsistent with Regulation S-P. Data security compliance is more than simply having a policy document. OCIE explained that written policies and procedures under Regulation S-P 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." Thus, the general approach for advisors and brokers-dealers should be to assess the threats and vulnerabilities to customer records and information, and then craft administrative, physical, and technical policies and procedures to address those threats and vulnerabilities.

OCIE also detailed data security practices that it found troubling under Regulation S-P. Examples include:

- **Personal devices** – employees storing and maintaining customer information on their personal laptops without policies and procedures address how to protect the information on those devices.
- **Electronic communications** – the absence of policies designed to prevent employees from regularly

sending unencrypted emails to customers containing PII.

- **Training and monitoring** – a lack of training for employee about encryption, password-protection, and transmission of PII through company-approved methods.
- **Outside vendors** – advisors and broker-dealers maintaining policies that required outside vendors to contractually agree to keep customers' PII confidential, but not following their own policies.
- **PII inventory** – not maintaining an inventory of all systems on which PII is maintained leaving advisors and broker-dealers unaware of the categories of customer PII that they maintain, and limiting the ability to adequately safeguard customer information.
- **Incident response plans** – plans failed to address role assignments for implementing the plan, actions required to address a cybersecurity incident, and assessments of system vulnerabilities.
- **Departed employees** – former employees of advisors and broker-dealers retained access to restricted customer information rights after termination of employment.

Many of the observations noted above are common gaps to data security policies and procedures, particularly for small and medium-sized enterprises in any industry. For advisors and broker-dealers, the consequences of compliance lapses could result in data breaches, enhanced scrutiny by the SEC and OCIE, and reputational harm. Thus, as OCIE suggests following its recent examinations, advisors and broker-dealers should review and update, as needed, their written policies and procedures to mitigate the issues identified by OCIE staff.

Source URL: https://www.natlawreview.com/article/sec-issues-privacy-and-data-security-risk-alert