KPMG

Regulatory Alert

Financial Services Regulatory Insight Center

April 2019

SEC Privacy Notice and Safeguards Policies

KPMG is issuing this Regulatory Alert to highlight ongoing attention to privacy issues and draw attention to the SEC's Risk Alert on Regulation S-P (Privacy of Consumer Financial Information).

Key points

- Regulatory approaches to data security and data privacy are actively being considered at the federal, state, and global level; this is an area of heightened attention.
- The SEC has issued a Risk Alert to highlight for investment advisers and broker-dealers its expectations regarding customer privacy notices and the safeguarding of customer records and information. Attention to these issues is consistent with the SEC's Examination Priorities.

The SEC's Office of Compliance Inspections and Examinations has issued a Risk Alert outlining compliance issues identified in examinations of SEC-registered investment advisers and brokers and dealers (collectively, Firms) related to Regulation S-P (Privacy of Consumer Financial Information). The alert focuses on the rule's i) privacy and opt-out notice provisions, and ii) requirements around written policies and procedures for safeguarding customer records and information (Safeguards Rule).

The following are among the most common Regulation S-P compliance issues:

- **Providing complete and accurate privacy and opt-out notices**. Some registrants did not provide Initial privacy notices, Annual privacy notices, or Opt-out notices to their customers. In cases where notices were provided, the notices did not accurately reflect the Firm's policies and procedures or provide notice of all of the customer's opt-out rights.
- **Lack of policies and procedures**. Some registrants did not have written policies and procedures that addressed all requirements of the Safeguards Rule, including administrative, technical, and physical safeguards for the protection of customer records and information.
- **Policies not implemented or reasonably designed to safeguard customer records and information**. Some registrants did not implement or reasonably design policies for customer records and information to i) ensure security and confidentiality, ii) protect against any anticipated threats or hazards to security or integrity, and iii) protect against unauthorized access or use that could result in substantial harm or inconvenience to the customer. SEC staff observed deficiencies or weaknesses in policies and procedures related to:
  - Storing or maintaining customer information on employee personal devices.
  - Clarifying the treatment of customer personally identifiable information (PII) in electronic communications.
  - Restricting the locations to where customer PII may be sent.

- Requiring an inventory of systems where customer PII is maintained.
- Storing or maintaining customer PII in unsecure physical locations.
- Limiting systems access, including the access of former employees.
- Holding outside vendors to the same compliance requirements.
- Developing incident response plans covering role assignments, required actions, or assessments of systems vulnerabilities.
- Monitoring to assess compliance or providing sufficient support (e.g., training) to allow employees to comply.

The SEC encourages Firms to review their written policies and procedures as well as their implementation of the policies and procedures to ensure compliance with Regulation S-P.

KPMG Perspectives

The SEC's 2019 Examination Priorities include a focus on retail investors and cybersecurity, highlighting access rights and controls, data loss prevention, vendor management, training, and incident response (see related KPMG Regulatory Alert here).

While the SEC's Risk Alert does not highlight any new provisions or expectations, it does reinforce that SEC examiners will be taking seriously Firms' efforts to protect customer PII. In addition, the Risk Alert clarifies the types of issues it will look for in examinations along with its expectation that Firms will have written policies and procedures and that those policies and procedures will be implemented as written.

Data security and data privacy are top of mind for regulators and consumers across all industries. High profile data breach and data sharing incidents have placed a spotlight on how consumer data is shared and utilized. Consumers now have a heightened awareness of the value in their personal information and are concerned about its collection, use, and retention. Public policy attention is focused on enhancing data governance and consumer protection frameworks (see KPMG's recent Regulatory Alert on regulatory attention to data privacy and enforcement here).

For additional information please contact Bill Meehan (Capital Markets), Charlie Jacco (Cybersecurity) or Perry Menezes (Cybersecurity).

Amy Matsuo
Principal and National Lead
Regulatory Insights
T: 919-664-7302
E: amatsuo@kpmg.com

Contributing authors:
Amy Matsuo, Principal and National Lead, Regulatory Insights

Karen Staines, Director, Financial Services Regulatory Insight Center

kpmg.com/socialmedia