April 25, 2019

Not So Secure: OCIE Identifies Regulation S-P Compliance Issues

On April 16, the SEC's Office of Compliance Inspections and Examinations (OCIE) published a Risk Alert outlining issues related to compliance with Regulation S-P that it identified in its inspections of SEC-registered investment advisers and brokers-dealers (Registrants).[1]

Regulation S-P

Regulation S-P generally requires a Registrant to provide customers with a clear and conspicuous privacy notice that accurately reflects the Registrant's privacy practices; the privacy notice must be provided when a customer relationship is established and, at least, annually. Registrants must also provide an opt-out notice explaining customers' right to opt-out of certain disclosures of their personally identifiable information (PII) to third parties.[2] The "Safeguards Rule" of the Regulation also requires Registrants to implement policies and procedures that include administrative, technical and physical measures designed to (1) ensure the security and confidentiality of customer information, (2) protect against any threats to the security or integrity of the information, and (3) protect against any unauthorized access to or use of the information.[3]

OCIE's Findings

The most frequent compliance issues noted were:

- ***Privacy and Opt-out Notices.*** Some Registrants either did not provide the notices required under the Regulation, or where notice was provided, the notices did not accurately reflect Registrants' policies and procedures.
- ***Policies and Procedures.*** Similarly, many Registrants either did not implement the required policies and procedures, or the policies and procedures in place were sufficiently lacking in that they "contained numerous blank spaces."
- ***Implementation and Safeguards.*** Where Registrants had implemented written policies and procedures, some of those policies and procedures were not designed to adequately secure customer information. Specifically, Registrants failed to:
  - Protect customer information stored on employees' personal devices;
  - Address and prevent personnel from sending unencrypted emails containing PII;
  - Appropriately train personnel on the use of encryption, password protection and use of approved methods of transmission, and monitor that the policies were being followed;

[1] https://www.sec.gov/files/OCIE Risk Alert - Regulation S-P.pdf.

[2] *See* 17 CFR 248.4-5, 7.

[3] *See* 17 CFR 248.30(a).

For more information, please contact your Katten attorney or any of the following:

Doron S. Goldstein
+1.212.940.8840
doron.goldstein@kattenlaw.com

Susan Light
+1.212.940.8599
susan.light@kattenlaw.com

Wendy E. Cohen
+1.212.940.3846
wendy.cohen@kattenlaw.com

Henry Bregstein
+1.212.940.6615
henry.bregstein@kattenlaw.com

Allison C. Yacker
+1.212.940.6328
allison.yacker@kattenlaw.com

David Y. Dickstein
+1.212.940.8506
david.dickstein@kattenlaw.com

Michael T. Foley
+1.312.902.5452
michael.foley@kattenlaw.com

- Prohibit personnel from sending customer PII to unsecure locations;
- Follow their own policies and procedures when engaging vendors, including failing to require vendors to agree to keep PII confidential;
- Identify all systems containing customer PII;
- Fully-develop incident response plans, including defining roles and responsibilities, and assessing system vulnerability;
- Keep PII in secure locations;
- Limit access to customer login credentials; and
- Terminate access rights of former employees.

Key Takeaways

The SEC continues to focus on cybersecurity, and the OCIE findings indicate that many Registrants are falling short of their obligations under Regulation S-P. OCIE made clear that compliance is more than just having a policy on paper that uses the Regulation's language: policies and procedures must accurately reflect practices and be implemented effectively throughout Registrants' operations. Doing so requires bringing together the appropriate resources—legal, compliance, operational and information technology—to review and update current policies and operations and to ensure that all personnel are trained on their responsibilities.