

**Alert | Financial Regulatory & Compliance/
Data, Privacy & Cybersecurity**



May 2019

OCIE Provides Registered Advisers and Broker-Dealers Guidance on Data Protection Compliance Obligations Under Reg S-P and Safeguards Rule

On April 16, 2019, the Securities and Exchange Commission’s Office of Compliance, Inspections and Examinations (SEC OCIE) issued a helpful **Risk Alert** relating to the privacy **Regulation S-P** (Reg S-P) and “**Safeguards Rule**” policies and procedures of registered investment advisers and broker dealers. The Risk Alert gives registered investment advisers and broker-dealers fair notice of various points of emphasis the SEC OCIE considers important from an examination perspective and those points that could surface post-breach when the SEC OCIE’s antennae are well-tuned towards finding fault with the registrant’s data protection practices.

After recounting the basics of Reg S-P’s privacy requirements and the requirements of the Safeguards Rule, the SEC OCIE lists what it calls “examples” of the “most common deficiencies or weaknesses identified by OCIE staff in connection with the Safeguards Rule.”

- A. Privacy and Opt-Out Notices – inaccurate (or completely absent) initial privacy notices, annual privacy notices, annual privacy notices, and/or opt-out notices provided to customers.
- B. Lack of policies and procedures under the Safeguards Rule, related to administrative, technical, and physical safeguards – though there are some policies that address the contents of the privacy notice, there are many that do not address written policies and procedures required by the Safeguards Rule.

- C. Policies not implemented or not reasonably designed to safeguard customer records and information – the SEC OCIE staff observes many registrants with written policies and procedures that are not implemented or not reasonably designed to (1) ensure the security and confidentiality of customer records and information, (2) protect against anticipated threats or hazards to the security or integrity of customer records and information, and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to customers. The SEC OCIE also notes general absence of the following:
- Policies and procedures that appear reasonably designed to safeguard customer information on personal devices like laptops;
 - Policies and procedures addressing the inclusion of customer personally identifiable information (PII) in electronic communications like unencrypted emails;
 - Policies and procedures prohibiting employees from sending customer PII to unsecured locations outside the registrant’s networks;
 - Policies and procedures followed by registrants requiring vendors to keep customer PII safe;
 - Policies and procedures identifying all systems where the registrant maintains customer PII, limiting the registrant’s ability to adopt reasonably designed policies and procedures to safeguard customer information;
 - Properly configured incident response plans, and procedures requiring the assessment of system vulnerabilities; and
 - Properly configured access management plans disabling former employees from logging into the network after they depart the firm so they cannot access restricted customer information.

Organizations concerned about whether their current data protection program complies with Reg S-P and the Safeguards Rule should consider a third-party gap analysis of their current program and regular vulnerability assessments.

For many of the issues identified by the SEC OCIE, the adage “pay me now or pay me later” comes to mind. Given that data breaches of large organizations are reported daily in journals and blogs, such organizations should generally be prepared for the worst. If a breach occurs and customer information is stolen, the SEC will likely take an exceedingly unsympathetic view if the registrant is found to have ignored well-defined guidance around the privacy and safeguarding of customer data.

Author

This GT Alert was prepared by **Paul Ferrillo**. Questions about this information can be directed to:

- **Paul Ferrillo** | +1 212.801.6598 | ferrillo@gtlaw.com
- **Ian C. Ballon** | +1 650.289.7881 | ballon@gtlaw.com
- **Dr. Viola Bensinger** | +49 30.700.171.150 | viola.bensinger@gtlaw.com
- **Kate Black** | +1 415.655.1300 | blackk@gtlaw.com
- **Lori Chang** | +1 310.586.3863 | changl@gtlaw.com
- **Francoise Gilbert** | +1 650.804.1235 | gilbertf@gtlaw.com
- **David M. Greenberg** | +1 212.801.6545 | greenbergdm@gtlaw.com

- Carsten Kociok | +49 30.700.171.119 | carsten.kociok@gtlaw.com
- Carmina Mogollón González | +52 55.5029.0034 | mogollonc@gtlaw.com
- Gretchen A. Ramos | +1 415.655.1319 | ramosg@gtlaw.com
- Radboud Ribbert | +31 (0) 20.301.7333 | ribbertr@gtlaw.com
- Alan N. Sutin | +1 212.801.9286 | sutina@gtlaw.com
- Hans Urlus | +31 (0) 20.301.7324 | urlush@gtlaw.com
- Or your Greenberg Traurig attorney

Albany. Amsterdam. Atlanta. Austin. Boca Raton. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany.~ Houston. Las Vegas. London.* Los Angeles. Mexico City.+ Miami. Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.* Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. ~Greenberg Traurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ¢Greenberg Traurig Tokyo Law Offices are operated by GT Tokyo Horitsu Jimusho, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by Greenberg Traurig Grzesiak sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in Greenberg Traurig Grzesiak sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2019 Greenberg Traurig, LLP. All rights reserved.*