SEC Office of Compliance Inspections and Examinations Issues Cybersecurity Preparedness Risk Alert

On April 15, 2014 the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert providing additional information concerning its initiative to assess cybersecurity preparedness in the securities industry.

The Risk Alert announces OCIE's plans to conduct examinations of more than 50 registered broker-dealers and registered investment advisers, focusing on areas related to cybersecurity. According to the Risk Alert, the focus areas of OCIE's examinations reportedly will include: the entity's cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats.

Notably, a sample document request list included in the Appendix to the Risk Alert telegraphs the types of documents and information that OCIE examiners might be interested in learning about, including:

- Identification of the persons responsible for managing the firm's information security assets and the frequency with which those practices are employed by the firm.
- A copy of the firm's written information security policy.

- The measures that firms take to protect IT assets (i.e., hardware, software and other network resources).
- If customers have remote on-line access or if the firm handles electronic funds transfer requests, what authentication and security measures are used by firms or their vendors to protect against risks such as hacking or identity theft.
- Policies and procedures addressing cybersecurity risks posed by third party vendors or business partners with access to firm networks, customer data or other sensitive information.
- Practices employed to detect unauthorized activity on firm networks or devices.
- Whether firms have updated their written supervisory procedures to reflect the Identity Theft Red Flags Rules, which became effective in 2013 (17 CFR § 248–Subpart C–Regulation S-ID) and which require broker-dealers and registered investment advisers that offer or maintain one or more "covered accounts" to "develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account" appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

A copy of the Risk Alert and accompanying Appendix is located here.