Proskauer

SEC to Conduct Second Round of Cybersecurity Examinations

September 16, 2015

On September 15, 2015, the Office of Compliance Inspections and Examinations (OCIE) of the Securities and Exchange Commission (SEC) issued a Risk Alert announcing its second round of examinations of registered investment advisers and broker-dealers under its cybersecurity examination initiative.

The OCIE's cybersecurity examination initiative was launched in April 2014 to assess cybersecurity preparedness in the securities industry and gather information on common practices and trends among registered firms. In its first round of examinations, the OCIE interviewed key personnel and reviewed documents of over 100 registered investment advisers and registered broker-dealers. Findings from this first round of examinations were released in February 2015. Whereas the first round of examinations consisted primarily of interviews and document reviews, the OCIE expects that the second round of examinations will involve more testing to assess implementation of a firm's procedures and controls. The examinations are expected to focus on the following key areas:

- **Governance and Risk Assessment.** The OCIE may assess whether the firm has cybersecurity governance and risk assessment processes on the key areas listed below, whether the firm is periodically evaluating its cybersecurity risks and whether the firm's controls and processes are tailored to its business. In addition, the OCIE may review the level of communication to, and involvement of, senior management and directors.
- **Access Rights and Controls.** The OCIE may review how the firm controls access to various systems and data via management of user credentials, authentication and authorization methods (including a review of the firm's controls associated with remote access, client logins, passwords, firm protocols to address client login problems, network segmentation and tiered access).

Data Loss Prevention. The OCIE may assess how the firm monitors the volume of content transferred outside of the firm by its employees or through third parties (such as by email attachments or uploads) and how the firm monitors for potentially unauthorized data transfers. It may also review how a firm verifies authenticity of client requests to transfer funds.

- **Vendor Management.** The OCIE may review the firm's practices and controls for vendor management (such as due diligence relating to vendor selection, monitoring and oversight, and contract terms). It may also evaluate how vendor relationships are handled as part of the firm's ongoing risk assessment process and how the firm determines the appropriate level of due diligence to conduct on a vendor.
- **Training.** The OCIE may look at how training is tailored to specific job functions and is designed to encourage responsible employee and vendor behavior. The OCIE may also review how procedures for responding to cyber incidents under an incident response plan are incorporated into personnel and vendor training.
- **Incident Response.** The OCIE may assess whether the firm has established policies, assigned roles, assessed system vulnerabilities and developed plans to address possible future incidents (including determining which firm data, assets and services warrant the most protection against attacks).

Registered investment advisers and broker-dealers should note that the areas of focus highlighted in the Risk Alert are not exhaustive and that OCIE examiners may select other areas of focus based on risks identified during the course of examinations. To assist firms in evaluating their cybersecurity preparedness, the OCIE has included a sample document request as an appendix to its Risk Alert.

This latest announcement reaffirms the SEC's continued focus on cybersecurity preparedness. Registered investment advisers and broker-dealers should evaluate their cybersecurity policies and procedures, as well as their implementation, in light of the Risk Alert and the sample document request. We note that the National Futures Association has also recently proposed cybersecurity requirements for its members. If you have any questions regarding the OCIE's examinations or cybersecurity issues in general, please contact your usual contact at Proskauer or any of the Proskauer attorneys listed in this alert.

Related Professionals

- **Arnold P. May**
  Partner
- **Amanda H. Nussbaum**
  Partner
- **Scott S. Jones**
  Partner
- **Charles (Chip) Parsons**
  Partner
- **Bruno Bertrand-Delfau**
  Partner
- **Jamiel E. Poindexter**
  Partner
- **Marc A. Persily**
  Partner
- **Ira G. Bogner**
  Managing Partner
- **Sarah K. Cherry**
  Partner
- **Bruce L. Lieb**
- **Nigel van Zyl**
  Partner
- **Michael R. Suppappola**
  Partner
- **Timothy W. Mungovan**
  Chairman of the Firm
- **Mary B. Kuusisto**
  Partner
- **Niamh A. Curry**
  Partner
- **David W. Tegeler**
  Partner

- **David T. Jones**
  Partner
- **Howard J. Beber**
  Partner
- **Robin A. Painter**
  Partner
- **Christopher M. Wells**
  Partner
- **Stephen T. Mears**
  Partner