Proskauer

SEC to Conduct Cybersecurity Examinations of Registered Investment Advisers and Broker-Dealers

April 24, 2014

On April 15, 2014, the Office of Compliance Inspections and Examinations (OCIE) of the U.S. Securities and Exchange Commission (SEC) announced in a risk alert that it will conduct cybersecurity examinations of over 50 registered investment advisers and broker-dealers. The examinations are part of OCIE's initiative to assess cybersecurity preparedness in the securities industry and obtain information on the industry's recent experiences with certain types of cyber threats. This latest announcement affirms the SEC's increased interest in the cybersecurity preparedness of regulated firms, a concern which has been identified as an examination priority for 2014 and was the subject of an SEC roundtable held on March 26, 2014.[1]

Cybersecurity Examinations

To assist firms in their compliance efforts regarding cybersecurity preparedness, OCIE has included a sample document request in its risk alert. Based on these materials, it appears that cybersecurity examinations will target the following areas:

- Cybersecurity governance and 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.

Registered investment advisers and broker-dealers should note that the risk alert and sample document request do not purport to be all-inclusive and expect that OCIE will tailor its examination based on the specific circumstances of the firm. In addition, the risk alert does not specify when examinations are expected to begin and how much advance notice a firm selected for examination will receive.

Action Items

Registered investment advisers and broker-dealers, regardless of whether they are selected for examination, should assess their cybersecurity infrastructure and policies in light of the items covered in the risk alert and the sample document request. In addition, firms should develop a plan for regularly testing the adequacy of their cybersecurity infrastructure and policies. Firms should implement periodic training for firm personnel and, if applicable, third party vendors and business partners authorized to access firm networks. Firms should also document any compliance measures taken as well as cybersecurity threats encountered by them (including any remedial steps undertaken in response to such threats).

If you have any questions regarding OCIE's cybersecurity initiative and examinations, please feel free to contact your usual contact at Proskauer or any of the Proskauer attorneys listed in this alert.

[1] A list of OCIE's Examination Priorities for 2014 is available here. For more information on the recent cybersecurity roundtable, please visit the SEC's website.

Related Professionals

- **Amanda H. Nussbaum**
  Partner
- **Scott S. Jones**
  Partner
- **Charles (Chip) Parsons**
  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
- **Arnold P. May**
  Partner
- **Mary B. Kuusisto**
  Partner
- **David W. Tegeler**
- **Howard J. Beber**
  Partner
- **Robin A. Painter**
- **Christopher M. Wells**
- **Stephen T. Mears**
  Partner