Proskauer

SEC Releases Results of Cybersecurity Examination Sweep

February 6, 2015

On February 3, 2015, the Office of Compliance Inspections and Examinations (OCIE) of the U.S. Securities and Exchange Commission (SEC) issued a Risk Alert summarizing findings from its examinations of over 100 registered investment advisers and broker-dealers.[1] The examinations were conducted as part of the OCIE's cybersecurity examination initiative, announced in April 2014,[2] to assess cybersecurity preparedness in the securities industry and gather information on common practices and trends among registered firms.

Cybersecurity Examinations

As part of the initiative, the OCIE interviewed key personnel and reviewed documents at 49 registered investment advisers and 57 registered broker-dealers. Of those 49 investment advisers, nearly two-thirds had assets under management of over $500 million. Clients of the investment advisers were largely retail investors, while roughly 15% were private funds. Over two-thirds of the investment advisers reported having custody of client funds and assets. The OCIE focused on how registered investment advisers and broker-dealers:

- Identify cybersecurity risks;
- Establish cybersecurity policies, procedures and oversight processes;
- Protect their networks and information;
- Identify and address risks associated with remote access to client information, funds transfer requests and third-party vendors; and
- Detect and handle unauthorized activities and other cyber-attacks.

The OCIE stated that the examinations were designed to discern differences in the level of cybersecurity preparedness among the examined firms. While the OCIE examined the accuracy of the firms' responses and the extent to which policies and procedures were implemented, it did not test the technical sufficiency of the firms' cybersecurity programs.

Summary Observations

Below are certain key findings regarding the examined investment advisers:

- Over 80% of investment advisers have adopted written cybersecurity policies. However, less than 15% of investment advisers address how the firm will determine if it is responsible for client cyber-related losses. Over half of the investment advisers base their policies and procedures on external models, such as the frameworks drafted by the National Institute of Standards and Technology, the International Organization for Standardization or the Federal Financial Institutions Examination Council.
- Nearly 80% of investment advisers conduct periodic firm-wide risk assessments. Around one-third also require the same of vendors that have access to the firms' networks.
- Over 70% of investment advisers have experienced cyber-related attacks, whether directly or indirectly through vendors. The majority of the cyber-related incidents were due to malware and fraudulent emails.
- While a few investment advisers reported using information-sharing networks as a resource for gathering information on cybersecurity attacks and practices, investment advisers more frequently relied on discussions with industry peers, conferences and independent research.
- The majority of investment advisers conduct firm-wide inventorying, cataloguing or mapping of their technology resources, including physical devices and systems, software platforms and applications, network resources, connections and data flows, connections from external sources to firm networks, hardware, data and software, and logging capabilities and practices.

Less than a quarter of the investment advisers incorporate cybersecurity requirements into their contracts with vendors and business partners. In addition, less than 15% maintain policies and procedures on information security training for vendors and business partners authorized to access their networks.

- In contrast to the broker-dealers examined, only a third of the investment advisers designate a Chief Information Security Officer. Instead, investment advisers typically delegate the responsibility to their Chief Technology Officer or assign another senior officer (i.e., Chief Compliance Officer, Chief Executive Officer or Chief Operating Officer) to liaise with a third-party consultant.
- While a majority of broker-dealers maintain insurance for cybersecurity incidents, only approximately 20% of investment advisers do so.

Registered investment advisers and broker-dealers should note that the OCIE is conducting further studies of cybersecurity preparedness among registered firms and has identified cybersecurity as one of its examination priorities for 2015. Registered investment advisers and broker-dealers should evaluate their cybersecurity policies and procedures in light of the observations in the Risk Alert. If you have any questions regarding the OCIE's examinations or cybersecurity issues in general, please feel free to contact your usual lawyer at Proskauer or any of the Proskauer lawyers listed in this alert.

[1] The SEC also released an Investor Bulletin providing online security tips to protect investor accounts from fraud.

[2] Please see our April 24, 2014 client alert for more information on the announcement.

Related Professionals

- **Arnold P. May**
  Partner
- **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
- **Timothy W. Mungovan**
  Chairman of the Firm
- **Mary B. Kuusisto**
  Partner
- **Malcolm B. Nicholls III**
  Partner
- **David W. Tegeler**
- **Howard J. Beber**
  Partner
- **Robin A. Painter**
- **Stephen T. Mears**
  Partner