The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 28707

February 3, 2015

SEC Publishes Risk Alert Containing Observations from OCIE's Recent Cybersecurity Review of Broker-Dealers and Advisers

[28707]

February 3, 2015

TO:

CHIEF INFORMATION SECURITY OFFICER ADVISORY COMMITTEE
CHIEF RISK OFFICER COMMITTEE No. 3-15
BROKER/DEALER ADVISORY COMMITTEE No. 5-15
SEC RULES MEMBERS No. 7-15
COMPLIANCE MEMBERS No. 5-15
SMALL FUNDS MEMBERS No. 3-15
TECHNOLOGY COMMITTEE No. 3-15
TRANSFER AGENT ADVISORY COMMITTEE No. 6-15
OPERATIONS MEMBERS No. 5-15
INTERNAL AUDIT ADVISORY COMMITTEE No. 2-15

RE:

SEC PUBLISHES RISK ALERT CONTAINING OBSERVATIONS FROM OCIE'S RECENT CYBERSECURITY REVIEW OF BROKER-DEALERS AND ADVISERS

As you may recall, last year the SEC's Office of Compliance Inspections and Examinations (OCIE) announced plans to conduct a review of cybersecurity preparedness in the securities industry. [1] Earlier today OCIE published a Risk Alert containing summary observations from its cybersecurity sweep, which involved an examination of 57 broker-dealers and 49 registered investment advisers to better understand how broker-dealers and advisers address the legal, regulatory, and compliance issues associated with cybersecurity. The background of OCIE's sweep and its observations as set forth in the Risk Alert published today are briefly summarized below.

Background

In April 2014, prior to commencing its review, OCIE published a Risk Alert to provide industry registrants additional information concerning the sweep. [2] This Risk Alert included, as an attachment, an Appendix that listed the types of information and documents that OCIE would request as part of its initiative. In light of the limited number of firms that OCIE planned to visit, OCIE hoped that the Appendix would provide registrants that were not visited as part of the sweep the opportunity to assess their own systems and processes against OCIE's expectations.

Summary of Observations from OCIE's Sweep

Scope of the Sweep

As noted above, OCIE's cybersecurity sweep involved an examination of 57 registered broker-dealers and 49 registered investment advisers. Today's Risk Alert summarizes OCIE's observations based on the sweep. According to Appendix B to the Risk Alert, [3] in terms of the nature of the clients served by the 49 advisers visited: 63.3% were primarily advisers to retail or individual clients; 14.3% were advisers to private funds; 12.2% were advisers to registered investment companies; 4.1% were advisers to pension funds; and 2.0% were advisers with diversified or institutional clients. In terms of their assets under management (AUM), 36.7% had AUM of less than $400 million; 36.7% had AUM of $401-900 million; and 26.5% had AUM in excess of $900 million. With respect to custody, 67% had custody of clients' funds or assets while 33% did not.

Focus of OCIE's Review

OCIE's focus in this sweep was on how the firms visited:

- 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 unauthorized activity.

The reviews were designed to discern basic distinctions among the level or preparedness of the firms visited. Importantly, OCIE's review did not include reviews of the registrants' technical sufficiency.

OCIE's Observations

According to the Risk Alert, OCIE observed the following during this review:

- The vast majority of examined broker-dealers (93%) and advisers (83%) have adopted written information security policies;
- The vast majority of firms examined conduct periodic risk assessments on a firm-wide basis to identify cybersecurity threats, vulnerabilities, and potential business consequences;
- Most of the firms visited reported that they have been the subject of a cyber-related incident. [Most of these involved malware or fraudulent emails];
- A majority of the firms have experienced cyber attacks directly or through one or

more of their vendors;
- Many examined firms identify best practices through information-sharing networks such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), which is described by registrants as “adding significant value in this effort;”
- The vast majority of examined firms report conducting firm-wide inventorying, cataloguing, or mapping of their technology resources;
- Almost all firms visited make use of encryption in some form;
- Many of the firms provide their clients with suggestions for protecting their sensitive information; and
- While 58% of the broker-dealers visited maintain insurance for cybersecurity incidents, only 21% of advisers maintain insurance that cover losses and expenses attributable to cybersecurity incidents. Of the firms visited, only one broker-dealer and one adviser reported filing claims under their cybersecurity policies.

Each of the above observations is discussed in more detail in the Risk Alert and the discussion includes information regarding differences between broker-dealers and advisers in each of these areas.

Also of note in the Risk Alert are differences among broker-dealers and investment advisers with respect to consideration of their vendors’ cybersecurity risk and the designation of Chief Information Securities Officers (CISOs). With respect the former, while 72% of broker-dealers incorporate requirements relating to cybersecurity risk into their contracts with vendors and business partners, only 24% of advisers do so. Also, while 51% of broker-dealers maintain policies and procedures related to information security training for vendors and business partners authorized to access their networks, only 13% of advisers do so. With respect to CISOs, while 68% of broker-dealers had an individual assigned as the firm’s CISO, only 30% of advisers have designated a CISO. More often, advisers either direct their Chief Technology Officer to take on the responsibilities typically performed by a CISO or they assign another senior officer (i.e., CCO, CEO, or COO) to liaise with a third-party consultant who is responsible for cybersecurity oversight.

Tamara K. Salmon
Associate General Counsel

endnotes

[1] See National Exam Program Risk Alert Volume IV, Issue 4 (February 3, 2015), which is available at: http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

[2] See National Exam Program Risk Alert Volume IV, Issue 2 (April 15, 2014), which is available at: http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf

[3] Appendix A provided a breakdown of the 57 registered broker-dealers by their number of registered representatives and by their category/peer group.