LOCKE LORD® QUICKStudy
Investment Adviser and Fund Management FUNDamentals™
February 9, 2015

SEC Issues Risk Alert on Cybersecurity

By: Heather M. Stone, Michael K. Renetzky and Matthew C. Dallett

On February 3rd, the Office of Compliance Inspections and Examinations (OCIE) of the Securities and Exchange Commission released a summary of its cybersecurity findings during sweep reviews in 2014. The sweep exams covered a cross section of more than 100 firms of various types and sizes, about half of which were investment advisers. As part of each sweep exam, OCIE analyzed each firm's awareness of cybersecurity issues and "culture of compliance" generally, as well as the firm's specific policies and procedures on cybersecurity issues. The OCIE reviewed each firm's procedures for identifying cybersecurity risks, the firm's choice of hardware and software to protect client information, the firm's ability to identify and evaluate cyber risks presented by its day-to-day operations (such as those posed by the use of third-parties, remote access and external fund transfer requests), and each firm's perceived ability to detect and prevent unauthorized activity. A substantial majority of the firms that were examined reported some exposure to one or more cyber-related incidents, most often stemming from some type of malware or fraudulent email.

The following is a short summary of each of the OCIE's focus areas when conducting the sweep reviews, as well as its findings.

- Identification of internal and external risks. The OCIE found that most investment advisers (over 75 percent) conduct periodic risk assessments to identify cybersecurity threats and vulnerabilities, and assess likely consequences. However, far fewer firms (less than 35 percent) focused on external risks, such as those posed by third parties (i.e., vendors or other service providers) who may have access to the firm's networks. The OCIE found that less than 25 percent of advisory firms incorporate requirements relating to cybersecurity into their third party contracts, mandate information security training for third parties authorized to access their networks, or require third parties to perform periodic assessments of their own cybersecurity vulnerabilities, comply with the adviser's cybersecurity policies and procedures, or have their own cybersecurity policies with protections equivalent to those of the adviser.

- Written information security policies. The OCIE found that most investment advisers (over 80 percent) have written information security policies, and over half those with such policies modeled them, at least in part, on one or more published cybersecurity risk management standards such as those of the Federal Financial Institutions Examination Council, the National Institute of Standards and Technology, or the International Organization for Standardization. Over half of advisory firms conduct periodic compliance audits of their information security policies and procedures. The OCIE found that many investment advisers have business continuity plans that address business interruptions caused by a cyber-attack and the subsequent recovery, but the vast majority (over 85 percent) fail to address the level of the

adviser's responsibility for any client losses associated with such an attack.

- Protecting the system. The OCIE noted that many firms share ideas and identify best practices in this area through their participation in industry groups and associations. In addition, the OCIE found that over 90 percent of advisers use data encryption, but only about 30 percent of investment advisers have a designated chief security officer and an even smaller percentage (about 20 percent) purchase cybersecurity insurance products.

The full text of the OCIE's cybersecurity sweep exam findings is available here. The sweep reviews were conducted as part of the OCIE's cybersecurity initiative, which can be found here.

We will continue to closely monitor these issues and will provide future client updates. Please contact one of the partners below if you have any questions. This is *QuickStudy* is for guidance only and is not intended to be a substitute for specific legal advice. If you would like further information, please contact the Locke Lord LLP attorney responsible for your matters or one of the attorneys listed below:

Heather M. Stone | 617-951-3331 | heather.stone@lockelord.com
Michael K. Renetzky | 312-443-1823 | mrenetzky@lockelord.com
Matthew C. Dallett | 617-239-0303 | matt.dallett@lockelord.com