Chapman and Cutler LLP
Attorneys at Law · Focused on Finance®

Client Alert

Current Issues Relevant to Our Clients

April 30, 2015

SEC Provides Guidance on Cybersecurity to Investment Advisers and Funds

The staff of the Securities and Exchange Commission's (the "SEC") Division of Investment Management recently published guidance for registered investment advisers and registered investment companies related to cybersecurity preparedness in their business practices. The guidance provides the investment management industry with the staff's views on what measures advisers and funds may consider in addressing cybersecurity risk. This Client Alert summarizes the staff's recommendations. You can obtain a copy of the staff's guidance here.

The staff's guidance comes following an uptick in interest by the SEC in cybersecurity within the financial services industry. The staff of the SEC's Office of Compliance Inspections and Examinations recently completed a round of cybersecurity preparedness examinations of over one hundred registered broker-dealers and investment advisers, the results of which can be found here. In addition, in 2014 the SEC hosted a cybersecurity roundtable to highlight the importance of cybersecurity and the issues and challenges it raises for the financial services industry.

The staff made a number of recommendations to funds and advisers for promoting and reviewing their cybersecurity preparedness. First, in order to identify potential cybersecurity threats and vulnerabilities, the staff recommends firms conduct periodic assessments of:

1. the nature, sensitivity and location of information that the firm collects, processes and/or stores, and the technology systems it uses;
2. internal and external cybersecurity threats to and vulnerabilities of the firm's information and technology systems;
3. security controls and processes currently in place;
4. the impact should the information or technology systems become compromised; and
5. the effectiveness of the governance structure for the management of cybersecurity risk.

The staff also notes that firms that share networks with other affiliated entities may want to broaden the scope of their assessments to the entire corporate network.

Next, the staff recommends that firms develop and implement a strategy to prevent, detect and respond to cybersecurity threats. The staff identifies several elements of what could be included in an effective cybersecurity strategy, including controlling access to systems and data, data encryption, restricting the use of removable storage, monitoring for unauthorized access or removal of data, data backup and retrieval and the development of an incident response plan. The staff also notes that firms may wish to consider the use of vendors or other outside resources in establishing their cybersecurity strategy and also suggests participating in information sharing organizations, such as the Financial Services–Information Sharing Analysis Center.

Finally, the staff recommends that firms adopt written policies and procedures and training programs to provide employees adequate guidance to prevent, detect and respond to cybersecurity threats. The staff also suggests that firms may wish to educate their clients or investors about how to reduce their own exposure to cybersecurity threats.

The staff notes that, in addition to the business risks cyber threats pose to firms, cyber attacks or other events could cause affected firms to violate federal securities laws if they are not able to reasonably prevent, detect or respond to such an event. For example, certain types of cyber attacks could prevent an investment company from processing shareholder transactions. The staff reminds firms to consider their securities law obligations when assessing their own cybersecurity preparedness.

For More Information

To discuss any topic covered in this Client Alert, please contact a member of the Investment Management Group or visit us online at chapman.com.