WILMERHALE

SEC To Examine Cybersecurity Preparedness at More Than 50 Registered Broker-dealers and Investment Advisers

APRIL 22, 2014

On April 15, 2014, the Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) issued a "Risk Alert" announcing steps being taken by the OCIE to assess cybersecurity preparedness in the securities sector. The OCIE intends to conduct a detailed examination of cybersecurity preparedness of more than 50 registered broker-dealers and registered investment advisers.

The SEC's Risk Alert includes a sample list of cybersecurity preparedness questions and document requests that the OCIE may use to conduct the examinations. The questions, based in part on the Cybersecurity Framework issued by the National Institute of Standards and Technology in February, are detailed and seek information related to a wide range of cybersecurity issues, including information with respect to identification of risks/cybersecurity governance, protection of firm networks, risks associated with remote customer access and funds transfer requests, and detection of unauthorized activity. In addition, the questions ask registered entities for a detailed list of security incidents since January 1, 2013, ranging from incidents involving malware and network breaches to hardware/software malfunctions and other security incidents. For each incident, the entity is asked to explain if it reported the incident to law enforcement, FinCEN (through the filing of a Suspicious Activity Report), FINRA, a state or federal regulatory agency, or an industry or public-private organization facilitating the exchange of information about cybersecurity incidents and risks.

A copy of the alert, as well as the sample questions, can be found here.

The OCIE Risk Alert highlights the importance of cybersecurity generally, not only as an issue for companies, but also for investors and the economy as a whole. It suggests that the SEC will continue to take an active role in assessing cybersecurity risks that may affect the securities industry. Indeed, at a March 26, 2014 SEC-sponsored Cybersecurity Roundtable, all of the SEC commissioners emphasized the importance of responding to threats in the securities sector. Chair Mary Jo White noted that there is a "compelling need for stronger partnerships between the government and private sector" and described the SEC's role with regard to cybersecurity as focusing on disclosure of material information, protection of market-related systems and the protection of investors.

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Andre E. Owens

PARTNER

Chair, Broker-Dealer Compliance and Regulation Practice

Co-Chair, Securities and Financial Regulation Practice

andre.owens@wilmerhale.com

+1 202 663 6350

Yoon-Young Lee

SENIOR COUNSEL

yoon-young.lee@wilmerhale.com

+1 202 663 6720

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195