



May 14, 2014

CLIENT ALERT

SEC to Examine Cybersecurity Risks of Broker-Dealers and Investment Advisers

The Securities and Exchange Commission’s Office of Compliance Inspections and Examinations (OCIE) issued a National Exam Priority Risk Alert on April 15¹ that provides information concerning its initiative to assess cybersecurity preparedness in the securities industry. The Risk Alert follows the March 26 cybersecurity roundtable hosted by the SEC, during which Chair White stressed the SEC’s concerns about cybersecurity threats and the importance of this area to the “integrity of our market system and customer data protection.” Chair White also emphasized the “compelling need for stronger partnerships between the government and private sector” to address cyber threats.

OCIE’s cybersecurity initiative is designed to assess cybersecurity preparedness in the securities industry and to obtain information about the industry’s recent experiences with certain types of cyber threats. To this end, OCIE will conduct examinations of more than 50 registered broker-dealers and registered investment advisers, which will focus on the following areas:

- cybersecurity governance
- identification and assessment of cybersecurity risks
- protection of networks and information
- risks associated with remote customer access and funds transfer requests
- risks associated with vendors and other third parties
- detection of unauthorized activity, and

¹ A copy of the Risk Alert is available at <http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf>

- experiences with cybersecurity threats

To promote compliance and to share with the securities industry where it sees risk, OCIE included in the Risk Alert a sample request for information and documents that it will be using in its initiative, so that firms can better assess their level of cybersecurity preparedness (even if they are not among the firms being examined). The sample request for information and documents includes detailed questions in each of the foregoing seven areas. The Risk Alert states that the sample request is not all inclusive of the information OCIE may request and that OCIE will alter its requests for information and documents, depending on the particular circumstances of each firm.

Registered broker-dealers and investment advisers should evaluate their existing cybersecurity policies and procedures and prepare for greater scrutiny of those policies and procedures. A review of the sample information and document request suggests that the SEC is placing great importance on the need for firms to have written policies for cybersecurity risk management in place. We can assist you in setting up cybersecurity policies and procedures that are appropriate for the specific circumstances of your systems or information technology environment or in reviewing your existing policies.

Firms should take steps so they are prepared in the event of a cybersecurity examination by OCIE. Should you receive notice of examination regarding your cybersecurity environment, please contact the undersigned or your regular Warsaw Burstein attorney.

Frederick R. Cummings, Jr.	fcummings@wbcsk.com	(212) 984-7807
Marshall N. Lester	mlester@wbcsk.com	(212) 984-7849
Paul A. Lieberman	plieberman@wbcsk.com	(212) 984-7806
Stephen W. Semian	ssemian@wbcsk.com	(212) 984-7764
Kyle A. Taylor	ktaylor@wbcsk.com	(212) 984-7797
Meryl E. Wiener	mwiener@wbcsk.com	(212) 984-7731

Warsaw Burstein, LLP

© Warsaw Burstein, LLP, 2014. All rights reserved.

This memorandum was prepared as a service to clients and other friends of Warsaw Burstein to report on recent developments that may be of interest to them. The information in it is therefore general, and should not be considered or relied on as legal advice. Throughout this memorandum, "Warsaw Burstein" and the "firm" refer to Warsaw Burstein, LLP.