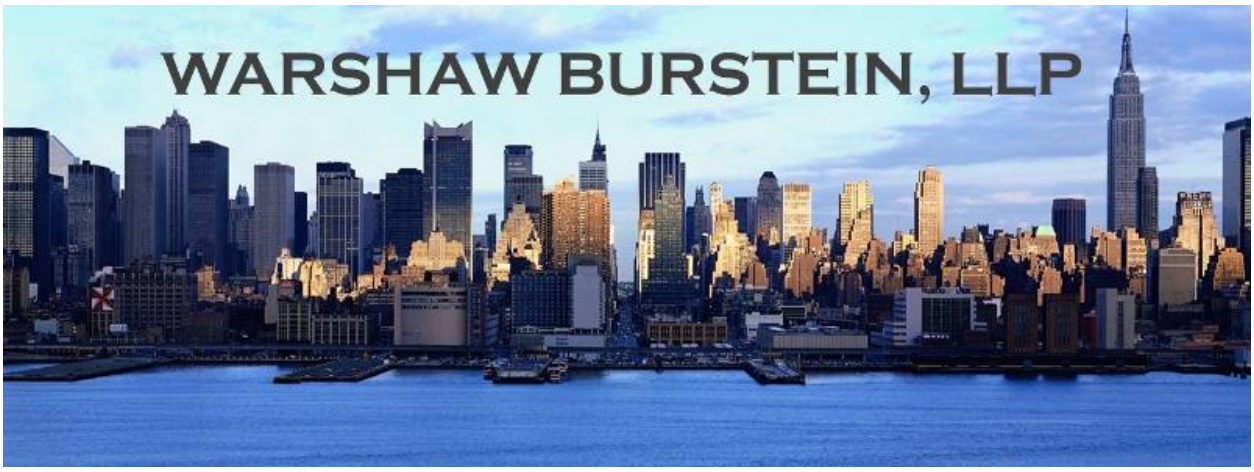

October 5, 2015

CLIENT ALERT

SEC Announces Additional Guidance on 2015 Cybersecurity Examination Initiative

The SEC's Office of Compliance Inspections and Examinations ("OCIE") issued a National Exam Program Risk Alert, dated September 15, 2015[*] (the "Risk Alert") that provides additional information on the areas of focus for OCIE's second round of cybersecurity examinations. This Risk Alert follows several previous risk alerts and a guidance update issued in April 2015, all of which were addressed by us in an earlier Client Alert that described the SEC's cybersecurity guidance following an initial round of cybersecurity examinations.[**] Following OCIE's initial round of cybersecurity examinations and its findings that highlighted some of the cybersecurity risk areas, the SEC issued this Risk Alert.

This Risk Alert provides additional information about a second round of examinations that will involve more testing to assess implementation of firm procedures and controls. The Risk Alert states that "[I]n light of recent cybersecurity breaches and continuing cybersecurity threats against financial services firms, the Cybersecurity Examination Initiative is designed to build on OCIE's previous examinations in this area and further assess cybersecurity preparedness in the securities industry, including firms' ability to protect broker-dealer customer and investment adviser client.….information."

The Risk Alert left no ambiguity that "[OCIE] examiners will gather information on cybersecurity-related controls and also will test to assess implementation of certain firm controls." The Risk Alert – as well as the included Appendix that sets forth a sample list of

[*] The full text of the Risk Alert is available at https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

[**] See our earlier Client Alert dated May 19, 2015.

information OCIE may request – identifies the following six areas of focus of the upcoming examination initiative:

- **Governance and Risk Assessment**

  Examiners may assess whether firms have in place cybersecurity governance and risk assessment processes, and whether firms are periodically evaluating cybersecurity risks to make sure that their controls are tailored to their businesses. Examiners also may review the involvement of senior managers and boards of directors in cybersecurity matters.

- **Access Rights and Controls**

  Examiners may review how firms control access to various systems and data via management of user credentials, authentication and authorization methods.

- **Data Loss Prevention**

  Examiners may assess how firms monitor the volume of content transferred outside the firm, such as by email attachments and how firms monitor for potentially unauthorized data transfers. Examiners also may verify the authenticity of customer requests to transfer funds.

- **Vendor Management**

  Examiners may focus on firm practices related to vendor management, including vendor selection and monitoring. In that connection, examiners may assess how vendor relationships are handled as part of the firm's ongoing risk assessment process and how the firm determines the appropriate level of due diligence to devote to the conduct of vendors.

- **Training**

  Examiners may focus on how training is tailored to specific employee job functions and how it is designed to encourage responsible employee behavior. Examiners also may review how training is updated to reflect cyber incidents.

- **Incident Response**

  Examiners may assess whether firms have established policies and plans, have assessed systems vulnerabilities, and have assigned roles to address possible cybersecurity breaches. Examiners also may focus on which firm data, assets and services warrant the most protection to help prevent cyber attacks from causing significant harm.

It should be noted, that these areas of focus are not exclusive and examiners may select additional areas on which to focus, based on risks they identify during the course of their examinations.

It would appear that this second round of cybersecurity examinations reflects the SEC's expectations that firms have in place policies and procedures to address, at the very least, the six focus areas identified. Firms should continue to reflect on their cybersecurity policies and procedures and adapt and update those policies and procedures, as needed.

*****

We are continuing to monitor cybersecurity issues. If you would like us to review and update your existing cybersecurity policies and procedures or would like us to prepare cybersecurity policies and procedures, please contact Meryl Wiener, any of the undersigned or your regular Warshaw Burstein attorney.

Frederick R. Cummings, Jr.	FCummings@wbcsk.com	(212) 984-7807
Thomas Filardo	TFilardo@wbcsk.com	(212) 984-7806
Marshall N. Lester	MLester@wbcsk.com	(212) 984-7849
Murray D. Schwartz	MSchwartz@wbcsk.com	(212) 984-7701
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