OCIE'S 2015 CYBERSECURITY EXAMINATION INITIATIVE

Date: 23 September 2015

Investment Management Alert

By: Mark C. Amorosi, Marguerite W. Laurent, András P. Teleki
, Arthur C. Delibert

On September 15, 2015, the Securities and Exchange Commission's ("SEC") Office of Compliance Inspections and Examinations ("OCIE") released a Risk Alert (the "2015 Risk Alert") that announced its second round of cybersecurity sweep examinations, summarized the topical focus areas of the examinations, and included a sample examination request letter (the "2015 Initiative"). OCIE conducted its first cybersecurity sweep initiative in 2014 (the "2014 Initiative"). The 2014 Initiative was announced April 15, 2014 in a Risk Alert that included a sample examination request letter, and culminated on February 3, 2015 in a Risk Alert with summary observations from OCIE's examinations of 57 registered broker-dealers and 49 registered investment advisers.

We believe the 2014 Initiative was a preliminary foray, focused on assessing the state of the market, that provided the SEC staff with the opportunity to create a baseline. In the 2014 sample examination request letter, the SEC staff asked for a detailed summary of all cybersecurity incidents that occurred at the examined firm over the previous year and general information relating to the firm's identification of risks and cybersecurity governance (including a list of the firm's three most serious cybersecurity risks), protection of firm 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 methodology for identifying best practices.

Unlike the 2014 Initiative, OCIE noted that the 2015 Initiative will focus more on evaluating a firm's implementation of systems called for by the firm's policies or systems that OCIE believes the firm should have. In the 2015 sweep examination, the SEC staff will collect information about an examined firm's cyber-related controls and then test whether, and how well, those controls have been implemented. At this stage, it appears the SEC staff intends to get to where the rubber meets the road, evaluating how prepared firms are to protect their cyber environment and to respond in the event of a breach. The SEC staff noted that "to promote better compliance practices and inform the [SEC's] understanding of cybersecurity preparedness," the 2015 Initiative will focus on six categories: governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.

While the tone of the 2015 Risk Alert implies that OCIE is "here to help" and primarily continuing its efforts to inform the SEC's understanding of the cybersecurity preparedness of the markets, we suggest firms be wary. Unlike the 2014 Initiative, the findings from this series of sweep examinations seem more likely to result in significant compliance deficiencies and, potentially, enforcement actions, in addition to another OCIE Risk Alert highlighting the SEC staff's observations. This possibility is heightened given OCIE's announced focus on actually testing and evaluating each examined firm's implementation of its cyber-related controls. It is further heightened by the IM Guidance Update on cybersecurity (the "2015 IM Guidance Update") that was published by

the staff of the SEC's Division of Investment Management earlier this year, in which the staff reminded investment advisers and mutual fund complexes of their compliance obligations in this area and set forth detailed guidance on the actions that investment management firms should be taking to address cybersecurity concerns.

The 2015 Risk Alert briefly highlights the questions on which the SEC staff may focus within each of the six broad categories when examining a firm. The sample examination request letter for the 2015 Initiative is broken into the same six categories and requests documents, such as relevant policies and procedures, contingency and business continuity plans, sample vendor notices, and related board minutes, as well as descriptions of incident response plan testing, incident alert systems, and any actual customer loss associated with recent incidents. Although the sample examination request letter is very focused on the written documents that act as the foundation for a firm's cybersecurity program, it is clear from the 2015 Risk Alert that the SEC staff intends to review those foundation documents and then test whether and how well the firm has implemented the documented program. We suspect that OCIE will not expect every firm to have fully implemented best practices across the board, but it will expect firms to be implementing logical, coherent, and well-thought-out programs that address their areas of significant exposure.

The 2015 Risk Alert specifically notes that while the six categories may represent the primary focus of the sweep examinations, the SEC staff may identify additional focus areas based on the risks identified during the course of the examinations. We also think that the SEC staff may have other areas of interest not listed in the 2015 Risk Alert. For example, the SEC staff may evaluate a firm's written policies and procedures surrounding system upgrades and software integration, and related planning and testing protocols, as well as the availability of back-up systems in the event an incident occurs during a planned upgrade. Further, the SEC staff may then evaluate how a firm implemented those policies and procedures during a recent upgrade or integration.

Every firm registered with the SEC in any capacity should be prepared in the event the SEC staff knocks on its door in the coming months to discuss cybersecurity. We encourage every firm to review the 2015 Risk Alert and the corresponding sample examination request letter, together with the 2014 Initiative Risk Alert, as well as the 2015 IM Guidance Update to evaluate and benchmark its cybersecurity preparedness against cybersecurity risks and conduct a self-assessment to gauge whether and how well your firm has implemented its documented cybersecurity program.

K&L Gates LLP maintains a Cybersecurity Task Force to assist clients in the evaluation and assessment of their cybersecurity risks, policies, and overall preparedness, as well as litigation of possible claims and charges and related insurance coverage issues. Please contact us if you would like to avail yourself of these services.

KEY CONTACTS

MARK C. AMOROSI
PARTNER

WASHINGTON DC
+1.202.778.9351
MARK.AMOROSI@KLGATES.COM

MARGUERITE W. LAURENT
PARTNER

WASHINGTON DC
+1.202.778.9403
MARGUERITE.LAURENT@KLGATES.COM

