Akin Gump
STRAUSS HAUER & FELD LLP

Cybersecurity, Privacy & Data Protection Alert

September 18, 2015

If you read one thing...

- On September 15th, the SEC OCIE announced in a Risk Alert it will launch a second round of cybersecurity examinations of registered broker-dealers and investment advisers, which will be more targeted than the prior sweep.
- The Risk Alert identifies specific areas of focus and also includes an appendix that provides a sample request for information and documents that firms should use to assess their own policies and procedures in advance of having to respond to the OCIE.
- The SEC specifically identified whether a firm's cybersecurity controls, preparation, vendor management and risk assessment processes are tailored to its business as potential areas of interest.

SEC OCIE Sharpens Focus on Cybersecurity

On September 15, 2015, the U.S. Securities and Exchange Commission (SEC) issued its latest Risk Alert in a series of alerts regarding cybersecurity. The Office of Compliance Inspections and Examinations (OCIE) announced that, "in light of recent cybersecurity breaches and continuing cybersecurity threats against financial services firms," as well as public reports of "cybersecurity breaches related to weaknesses in basic controls," it will launch a second round of examinations of registered broker-dealers and investment advisers. These examinations will be more targeted than the prior sweep, focusing on the six areas that pose the most significant risk.

This Risk Alert builds upon a report issued by the OCIE in February 2015, after it conducted its first round of cybersecurity examinations beginning in April 2014. That report highlighted some of the cybersecurity risk areas for investment advisers and broker-dealers. According to the latest Risk Alert, the OCIE elected to launch a second initiative in order to promote better compliance practices and further the SEC's understanding of cybersecurity preparedness.

The Risk Alert identifies specific areas of focus for the second round of cybersecurity examinations:

- Governance and Risk Assessment – Are firms periodically evaluating security risks and tailoring their controls to their business? Examiners may review the communications of senior management and the board of directors, including, but not limited to, board minutes and briefing materials, to assess

their involvement. Examiners may also seek information regarding a firm's chief information security officer, and other employees responsible for cybersecurity matters.

- Access Rights and Controls – Are firms updating access rights based on personnel or system changes? Examiners may review the controls associated with remote access, customer logins and passwords, such as use of multifactor authentication.
- Data Loss Prevention – Do firms have robust controls in the areas of patch management and system reconfiguration? Examiners may assess how firms monitor content transferred to and from the firm and the authenticity of customer requests to transfer funds.
- Vendor Management – Do firms have practices and controls in place related to the risk of hacking of third-party vendor platforms? Examiners may assess how vendors are selected and monitored.
- Training – Do firms have appropriate training programs in place? Examiners may assess how training is tailored to specific job functions, designed to encourage responsible employee behavior and updated to reflect cyber incidents.
- Incident Response – Do firms have established policies, assigned roles and developed plans to respond to cybersecurity attacks? Examiners may review information regarding breaches, losses and remediation, tests or exercises of the incident response plan and cyber insurance.

Key Takeaways

Firms should begin preparing now for this second round of examinations. The OCIE has attached to the Risk Alert a sample request for information and documents; firms can expect the OCIE to issue such requests in short order. Firms should use this sample request to assess their own policies and procedures in advance of having to respond to the OCIE.

Contact Information

If you have any questions regarding this alert, please contact:

Natasha G. Kohne
nkohne@akingump.com
+971 2.406.8520 - Abu Dhabi
+1 212.872.1000 – New York

Michelle A. Reed
mreed@akingump.com
+ 1 214.969.2713
Dallas

David S. Turetsky
dturetsky@akingump.com
+1 202.887.4074
Washington, D.C.

Isabelle R. Gold
igold@akingump.com
+1 212.872.7482
New York

Jo-Ellyn Sakowitz Klein
jsklein@akingump.com
+1 202.887.4220
Washington, D.C.

Prakash H. Mehta
pmehta@akingump.com
+1 212.872.7430
New York

Eliot D. Raffkind
eraffkind@akingump.com
+1 214.969.4667
Dallas