SEC Issues Cybersecurity Initiative

Skadden

09/21/15

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Anastasia T. Rockas
New York
212.735.2987
anastasia.rockas@skadden.com

Stuart D. Levi
New York
212.735.2750
stuart.levi@skadden.com

Cyrus Amir-Mokri
New York
212.735.3279
cyrus.amir-mokri@skadden.com

Four Times Square
New York, NY 10036
212.735.3000

skadden.com

On September 15, 2015, the U.S. Securities and Exchange Commission (the "SEC") issued a risk alert release announcing that the Office of Compliance Inspections and Examinations ("OCIE") will be conducting a new Cybersecurity Examination Initiative (the "Initiative").[1] Through the Initiative, OCIE will undertake a second round of examinations of registered broker-dealers and investment advisers' cybersecurity preparedness in light of recent breaches and continuing threats against financial services firms. The release highlights a number of areas of focus that the OCIE will cover when conducting their examinations.

Background

In March 2014, the SEC invited industry representatives to a cybersecurity roundtable to underscore the importance of cybersecurity to the integrity of the market system and customer data protection.[2] In April 2014, the OCIE published a risk alert announcing the examination of more than 50 registered broker-dealers and investments advisers, focusing on areas related to cybersecurity risks and preparedness.[3] A summary of OCIE's finding was published in February 2015, reflecting the legal, regulatory and compliance issues relating to cybersecurity.[4] OCIE announced a renewed focus on cybersecurity compliance and controls as part of its 2015 Examination Priorities and issued its most recent risk alert release to elaborate on the guidelines by which it will conduct its next round of examinations.[5]

Areas of Focus

In an effort to ensure that firms can adequately protect broker-dealer customer and investment adviser client information, OCIE will examine various cybersecurity-related controls and test implementation of those controls. The Initiative is designed to build on OCIE's prior cybersecurity examinations and will involve more testing to assess implementation of firm procedures and controls. The Initiative will focus on the following areas, many of which are consistent with areas of focus of other regulators:

- **Governance and Risk Assessment.** Examiners may assess whether registrants have cybersecurity governance and risk assessment processes in the areas set out below and whether those controls and processes are evaluated regularly and adequately tailored.
- **Access Rights and Controls.** Examiners will look at how firms control access to various systems and data via management of user credentials, authentication and authorization, including controls associated with remote access, customer logins and passwords.
- **Data Loss Prevention.** Examiners will assess how firms monitor the volume of content transferred outside of the firm by its employees or through third parties, such as by email attachments or uploads. This also will include an assessment of how firms monitor for unauthorized data transfers and how firms verify the authenticity of a customer request to transfer funds.
- **Vendor Management.** Examiners will study firm practices and controls related to vendor management, such as due diligence in selecting a vendor, monitoring and oversight of vendors and contract terms.

[1] OCIE, NEP Risk Alert, "OCIE's 2015 Cybersecurity Initiative" (September 15, 2015).
[2] Skadden, "SEC Holds Roundtable on Cybersecurity" (March 28, 2014).
[3] OCIE, NEP Risk Alert, "OCIE Cybersecurity Initiative" (April 15, 2014).
[4] OCIE, NEP Risk Alert, "Cybersecurity Examination Sweep Summary" (February 3, 2015).
[5] OCIE, "Examination Priorities for 2015" (January 13, 2015).

SEC Issues Cybersecurity Initiative

- **Training.** Examiners will focus on how training is tailored to specific job functions and designed to encourage responsible employee and vendor behavior, and will review procedures for responding to cyber incidents under an incident response plan.
- **Incident Response.** Examiners will assess whether firms have established policies, assigned roles, assessed system vulnerabilities and developed plans to address possible future events.

The Initiative includes a sample request for information and documents as an attachment.

Conclusion

In light of the OCIE's continued interest in promoting the Cybersecurity Examination Initiative, it would be prudent for broker-dealers and investment advisers to reflect on their cybersecurity policies and preparedness. Skadden's Privacy and Cybersecurity Group has the experience to assist clients in meeting these requirements.