SULLIVAN & CROMWELL LLP

August 11, 2017

OCIE Issues Risk Alert Following Recent Cybersecurity Examinations of Financial Firms

Office of Compliance Inspections and Examinations Summarizes Observations on Industry Practices and Identifies Continuing Areas of Weakness

SUMMARY

On August 7, 2017, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a risk alert (Risk Alert) summarizing the findings of recent examinations conducted as part of its 2015 Cybersecurity 2 Initiative.[1] Between September 2015 and June 2016, OCIE examined 75 financial firms registered with the SEC (including broker-dealers, investment advisers and investment companies) to assess industry practices and issues associated with the firms' cybersecurity preparedness. These examinations built upon prior cybersecurity examinations, particularly OCIE's 2014 Cybersecurity 1 Initiative. In general, OCIE staff observed increased cybersecurity preparedness but also identified areas where compliance and oversight could be improved. The Risk Alert summarizes the staff's observations from the examinations and highlights certain issues observed as well as certain policies and procedures that the staff believes may be effective. Cybersecurity remains a top compliance risk for financial firms, and OCIE has indicated that it will continue to examine cybersecurity procedures and controls.

While OCIE noted overall improvement in cybersecurity preparedness since the 2014 Cybersecurity 1 Initiative, it also identified several continuing areas of weakness. Specifically, the Risk Alert notes that firms may need to exert greater effort to ensure that their policies are being enforced. Given the attention that OCIE has devoted to cybersecurity compliance among financial firms in light of the growing cyber-related threats, financial firms should consider whether the vulnerabilities identified in the Risk Alert—or

other cybersecurity issues—may need to be addressed in order to update or strengthen their cybersecurity risk management systems.

KEY OBSERVATIONS

The staff noted an overall improvement in awareness of cyber-related risks and the implementation of certain cybersecurity practices since the 2014 examinations, most notably, that all broker-dealers, all funds and nearly all advisers examined maintained cybersecurity-related written policies and procedures addressing the protection of records and information. Nonetheless, the staff observed issues with the information protection policies and procedures or their implementation at a majority of the firms. Examples cited included (i) policies and procedures that were not reasonably tailored and provided employees only vague or over-generalized guidance and (ii) firms that did not appear to adhere to or enforce policies and procedures or where actual practice often differed from written policies and procedures. For instance, OCIE observed ongoing reviews being conducted less frequently than policies required and a lack of follow-up when employees failed to complete their cybersecurity training.

In the Risk Alert, the SEC also highlighted system maintenance inadequacies that may lead to non-compliance with Regulation S-P, emphasizing the importance of establishing and maintaining operational safeguards to protect customer records and information. OCIE observed, for example, problematic practices such as failures to install software patches to address security vulnerabilities, use of outdated operating systems that were incompatible with new security patches and delays in remediating high-risk findings from penetration tests or vulnerability scans.

The Risk Alert, however, also listed certain elements that were included in the policies and procedures of firms that the staff believed had implemented robust cybersecurity controls. These elements include: (1) maintaining a complete inventory of data, information and vendors; (2) providing detailed cybersecurity-related instructions; (3) maintaining prescriptive schedules and procedures for testing data integrity and vulnerabilities; (4) establishing and enforcing data access controls; (5) requiring periodic information security training for employees and ensuring completion of training; and (6) involving senior management in vetting cybersecurity policies. The SEC encouraged firms to consider these elements, as well as the Division of Investment Management's 2015 guidance on cybersecurity preparedness,[2] in ongoing evaluation and implementation of cybersecurity measures.

* * *

ENDNOTES

[1] Securities and Exchange Commission, Office of Compliance Inspections and Examinations, *National Exam Program Risk Alert: Observations from Cybersecurity Examinations* (Aug. 7, 2017), *available at* https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.

[2] *See* our client memo on the Division of Investment Management's 2015 guidance, *available at* https://www.sullcrom.com/siteFiles/Publications/SC_Publication_SECs_Division_of_Investment_Management_Releases_Cybersecurity_Guidance.pdf.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future related publications from Michael B. Soleta (+1-212-558-3974; soletam@sullcrom.com) in our New York office.

CONTACTS

New York		
John E. Baumgardner Jr.	+1-212-558-3866	baumgardnerj@sullcrom.com
Whitney A. Chatterjee	+1-212-558-4883	chatterjeew@sullcrom.com
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Donald R. Crawshaw	+1-212-558-4016	crawshawd@sullcrom.com
Elizabeth T. Davy	+1-212-558-7257	davye@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
William G. Farrar	+1-212-558-4940	farrarw@sullcrom.com
Nicole W. Friedlander	+1-212-558 4332	friedlandern@sullcrom.com
C. Andrew Gerlach	+1-212-558-4789	gerlacha@sullcrom.com
Nader A. Mousavi	+1-212-558-1624	mousavin@sullcrom.com
Frederick Wertheim	+1-212-558-4974	wertheimf@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com
Michael M. Wiseman	+1-212-558-3846	wisemanm@sullcrom.com
Washington, D.C.		
Eric J. Kadel, Jr.	+1-202-956-7640	kadelj@sullcrom.com
Samuel R. Woodall III	+1-202-956-7584	woodalls@sullcrom.com
Palo Alto		
Gary Israel	+1-650-461-5664	israelg@sullcrom.com
Nader A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com