WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

New SEC Enforcement Action Gives Force to Ongoing Safeguards Requirements

June 20, 2016

AUTHORS

Elizabeth P. Gray | James E. Anderson | William J. Stellmach | Ashley E. Singletary-Claffee

On June 8, 2016, the Securities and Exchange Commission (the "SEC") announced charges against Morgan Stanley Smith Barney LLC ("MSSB"), following a cyber breach involving MSSB customer data, for failing to adopt written policies and procedures reasonably designed to protect customer records and information under the Safeguards Rule of Regulation S-P. MSSB, a dually registered broker-dealer and investment adviser, paid a $1 million civil money penalty and agreed to a censure to settle the administrative proceeding.[1] Together with a prior settlement involving a data breach at R.T. Jones, the MSSB settlement signals the SEC's willingness to pursue punitive measures to ensure compliance with the Safeguards Rule and also suggests that any informal grace period for implementing its views on effective cybersecurity protocols by financial institutions previously outlined in Staff guidance will soon expire, if it has not already. This enforcement action also provides critical insight into the SEC's evolving interpretations of the Safeguards Rule and reinforces the SEC's recent messaging regarding cybersecurity and the safeguarding of customer information.

The Safeguards Rule requires registered broker-dealers and investment advisers to adopt written policies and procedures reasonably designed to: (1) insure the security and confidentiality of customer records and information; (2) protect against

[1] MSSB neither admitted nor denied the SEC's findings. *See* Morgan Stanley Smith Barney LLC, Investment Advisers Act Release No. 4,415 (June 8, 2016), *available* here.

any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

The MSSB case reinforces SEC Chair Mary Jo White's May 17, 2016 remarks in which she noted that cybersecurity is the biggest threat facing the global financial system.[2] The settlement is the second SEC enforcement action in the past 12 months alleging a violation of the Safeguards Rule on the basis of an investment adviser's weak cyber controls.[3] Previously, the SEC's views on effective cybersecurity protocols were articulated in a series of Staff guidance updates and examination findings.[4] In announcing the settlement, SEC Enforcement Director Andrew Ceresney reiterated that "the dangers and impact of cyber breaches" make data security "a critically important aspect of investor protection."[5]

The SEC's Cybersecurity Initiative

The MSSB settlement marks the latest in an escalating pattern of regulatory actions targeting cybersecurity controls among investment advisers and broker-dealers. In 2014 and 2015, the SEC's Office of Compliance Inspections and Examinations ("OCIE") conducted targeted examinations of broker-dealers and investment advisers that focused on cybersecurity governance and risk assessments, access rights and controls, data loss prevention, vendor management, training, and incident response.[6] As a result of the OCIE Cybersecurity Initiative in 2014, the SEC staff examined 57 registered broker-dealers and 49 registered investment advisers. In a Risk Alert summarizing its observations, OCIE noted that the vast majority of examined firms have adopted written information security policies and procedures and that most conduct periodic audits to determine compliance with these policies.[7] OCIE further identified that the vast majority of examined firms conduct periodic, firm-wide risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences, that almost all of the examined firms make use of some form of encryption, and that most of the examined firms reported that they have been the subject of a cyber-related incident.

---

2 *See* Lisa Lambert and Suzanne Barlyn, *SEC Says Cyber Security Biggest Risk to Financial System,* REUTERS (May 18, 2016), *available* here.

3 *See* R.T. Jones Capital Equities Management, Inc., Investment Advisers Act Release No. 4,204 (Sept. 22, 2015).

4 *See* IM Guidance Update, Cybersecurity Guidance (April 2015), *available here*; OCIE, National Exam Program, Risk Alert: Cybersecurity Examination Sweep Summary (Feb. 3, 2015), *available* here [hereinafter "Sweep Summary"]; *see generally* Cybersecurity Roundtable, SEC, *available* here (last modified May 11, 2016).

5 *See* SEC Press Release, "Morgan Stanley Failed to Safeguard Customer Data," *available* here.

6 *See* OCIE, National Exam Program Risk Alert: OCIE's 2015 Cybersecurity Examination Initiative (Sept. 15, 2015), *available here*; OCIE, National Exam Program Risk Alert: OCIE Cybersecurity Initiative (Apr. 15, 2014), *available* here.

7 *See* Sweep Summary.

Impact of Cybersecurity on Financial Services Firms

In September 2015, the SEC alleged that R.T. Jones Capital Equities Management, Inc. stored sensitive personally identifiable information of clients on a third-party-hosted server without adopting any written policies and procedures to ensure the security and confidentiality of the information and to protect it from anticipated threats or unauthorized access. Ultimately, the firm's web server was attacked in July 2013 by an unknown hacker who gained access and copy rights that rendered the personally identifiable information of more than 100,000 individuals, including thousands of R.T. Jones's clients, vulnerable to theft. In settling the case, the SEC also noted that R.T. Jones did not conduct periodic risk assessments, employ a firewall to protect the client information, encrypt the client information on the server, or establish procedures for responding to a cybersecurity incident.

Also, in August 2015, the SEC filed fraud charges against 32 defendants for participating in an international scheme in which hackers allegedly infiltrated newswire services and traded on corporate earnings announcements before they were released publicly, generating more than $100 million in illicit profits. According to press releases, the SEC coordinated its investigatory efforts with the Federal Bureau of Investigation, the Department of Homeland Security, the Financial Industry Regulation Authority, U.S. Attorney's Offices, and the United Kingdom Financial Conduct Authority, among other regulatory entities. The financial services sector, in particular, has been a popular target for hackers over the last several years. Most recently, in May 2016, the hacking collective Anonymous launched an attack against the Bank of Greece's website and threatened to target similar websites of other central banks around the world.

Here, the SEC alleged that from 2011 to 2014, an MSSB employee, Galen Marsh, misappropriated data concerning 730,000 customer accounts associated with 330,000 different households. The data included customers' full names, phone numbers, street addresses, account numbers, account balances and securities holdings. According to the SEC, MSSB maintained hundreds of computer applications to store the sensitive personally identifiable information, but Marsh importantly accessed only two portals, the Fixed Income Division Select Portal and the Business Information System Portal. Both portals suffered a similar flaw: neither limited Marsh's access to only information for customers for whom he was properly authorized. As a result, Marsh could run reports that contained the confidential information of vast numbers of customers throughout MSSB.

Although MSSB had written policies and procedures addressing customer information safeguards—including a policy restricting employee access to confidential information for a limited number of customers, the authorization modules described above, which operationalized the policy's restrictions, and technology controls that prevented employees from copying data onto removable storage devices and from accessing certain kinds of websites—the SEC found that MSSB failed to ensure that these policies and procedures were reasonably designed to meet the objectives of the Safeguards Rule. In particular, the SEC highlighted that: (1) the authorization modules were ineffective in limiting employee access to data; (2) MSSB failed to conduct audits or tests of the modules at any point in the 10 years since their creation; and (3) MSSB did not monitor user activity in the firm's applications that stored the personally identifiable information of its clients.

By the time MSSB discovered the breach during one of its routine Internet sweeps, Marsh had already transferred the customer data to a personal website. Subsequent forensic analysis identified that a third party likely hacked into that website's server and copied the customer information that Marsh had downloaded. The hacker then posted portions of the confidential data on the Internet with offers to sell larger quantities of the information.

In a separate SEC order, Marsh agreed to an industry bar with the right to apply for re-entry in five years. He was also criminally convicted for his conduct last year, sentenced to 36 months of probation, and was required to pay $600,000 in restitution.

In light of the SEC's heightened and increasingly aggressive scrutiny, broker-dealers and investment advisers who have not already done so should take care to make cybersecurity governance a key priority. Firms should institute robust written policies and procedures for safeguarding client information, specifically addressing the performance of regular cybersecurity risk assessments, strategies for preventing cybersecurity threats such as through the use of firewalls and encryption, and responses to data breaches and other cyber incidents. This recent enforcement action provides a partial road map for tailoring an effective and regulatory compliant data safeguard program, but firms need to conduct a timely self-assessment to evaluate both the technical and regulatory risks.

If you have any questions regarding this memorandum, please contact Elizabeth P. Gray (202-303-1207; egray@willkie.com), James E. Anderson (202-303-1114; janderson@willkie.com), William J. Stellmach (202-303-1130; wstellmach@willkie.com), Ashley E. Singletary-Claffee (202-303-1233; asingletary-claffee@willkie.com), or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

June 20, 2016