UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 78021 / June 8, 2016

INVESTMENT ADVISERS ACT OF 1940
Release No. 4415 / June 8, 2016

ADMINISTRATIVE PROCEEDING
File No. 3-17280

In the Matter of **Morgan Stanley Smith Barney LLC,** **Respondent.**	**ORDER INSTITUTING ADMINISTRATIVE AND CEASE-AND-DESIST PROCEEDINGS, PURSUANT TO SECTIONS 15(b) AND 21C OF THE SECURITIES EXCHANGE ACT OF 1934, AND SECTIONS 203(e) AND 203(k) OF THE INVESTMENT ADVISERS ACT OF 1940, MAKING FINDINGS, AND IMPOSING REMEDIAL SANCTIONS AND A CEASE-AND-DESIST ORDER**

I.

The Securities and Exchange Commission (the "Commission") deems it appropriate and in the public interest that public administrative and cease-and-desist proceedings be, and hereby are, instituted pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934 (the "Exchange Act"), and Sections 203(e) and 203(k) of the Investment Advisers Act of 1940 (the "Advisers Act"), against Morgan Stanley Smith Barney LLC ("MSSB" or "Respondent").

II.

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the "Offer"), which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission's jurisdiction over it and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, and Sections 203(e) and 203(k) of the Investment Advisers Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order ("Order"), as set forth below.

III.

On the basis of this Order and Respondent's Offer, the Commission finds[1] that:

Summary

1. This proceeding arises out of MSSB's failure to adopt written policies and procedures reasonably designed to protect customer records and information, in violation of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) (the "Safeguards Rule"). From at least August 2001 through December 2014, MSSB stored sensitive personally identifiable information ("PII") of individuals to whom MSSB provided brokerage and investment advisory services (referred to herein as "customers") on two of the firm's applications: the Business Information System ("BIS") Portal and the Fixed Income Division Select ("FID Select") Portal (collectively, "the Portals"). Galen Marsh ("Marsh"), then an MSSB employee, misappropriated data regarding approximately 730,000 customer accounts, associated with approximately 330,000 different households, by accessing the Portals between 2011 and 2014. The misappropriated data included PII, such as customers' full names, phone numbers, street addresses, account numbers, account balances and securities holdings.

2. Between approximately December 15, 2014 and February 3, 2015, portions of this stolen data were posted to at least three Internet sites along with an offer to sell a larger quantity of stolen data in exchange for payment in speedcoins, a digital currency. MSSB discovered the data breach through one of its routine Internet sweeps on December 27, 2014. After comparing certain data reports generated by Marsh to the information posted on the Internet, MSSB identified Marsh as the likely source of the data breach. On December 29 and 30, 2014, MSSB interviewed Marsh, who acknowledged that he had accessed and downloaded confidential customer data to his own data storage device (hereafter, "personal server"). Marsh denied posting any of the data on the Internet. Subsequent forensic analysis of Marsh's personal server revealed that a third party likely hacked into the personal server and copied the confidential customer data that Marsh had downloaded from the Portals.

3. The Safeguards Rule, which the Commission adopted in 2000 and amended in 2005, requires, among others, every broker-dealer and investment adviser registered with the Commission to adopt written policies and procedures reasonably designed to: (1) insure the security and confidentiality of customer records and information; (2) protect against 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. MSSB violated the Safeguards Rule because its policies and procedures were not reasonably designed to meet these objectives by failing to include, for example: reasonably designed and operating authorization modules for the Portals that restricted employee access to only the confidential customer data as to which such employees had a legitimate business need; auditing and/or testing of the

[1] The findings herein are made pursuant to Respondent's Offer of Settlement and are not binding on any other person or entity in this or any other proceeding.

effectiveness of such authorization modules; and monitoring and analysis of employee access to and use of the Portals.

Respondent

4. MSSB is a Delaware limited liability company and is registered with the Commission as a broker-dealer and an investment adviser. MSSB is an indirect wholly-owned subsidiary of Morgan Stanley and has its principal office and place of business in Purchase, New York.

Background

A. Confidential Customer Data at MSSB

5. In connection with its wealth management business, MSSB maintains hundreds of computer applications containing customers' PII. The two applications of relevance here are the BIS Portal and the FID Select Portal. The Portals were Web applications residing on MSSB's intranet that enabled certain MSSB employees to run reports that retrieved and organized customer data from underlying databases. At the relevant time, the BIS Portal could be used to run approximately 40 different reports, one of which was the Relationship Migration Book Analysis Report, which contained customers' full names, account numbers, phone numbers, states of residence and account balances.

6. The FID Select Portal was another Web application available on MSSB's intranet. This portal was used by MSSB Financial Advisors ("FAs"), who were usually the primary points of contact for customers, as well as the Client Service Associates ("CSAs") who supported the FAs, to obtain reports on the fixed income holdings in their customers' accounts. In particular, the Account Analysis Report available through the FID Select Portal provided customers' full names, account numbers, phone numbers, street addresses, account balances and information about specific fixed income holdings.

7. MSSB adopted certain policies and restrictions with respect to employees' access to and handling of confidential customer data available through the Portals. MSSB had written policies, including its Code of Conduct, that prohibited employees from accessing confidential information other than what employees had been authorized to access in order to perform their responsibilities. In addition, MSSB designed and installed authorization modules that, if properly implemented, should have permitted each employee to run reports via the Portals only with respect to the data for customers whom that employee supported. These modules required FAs and CSAs to input numbers associated with the user's branch and FA or FA group number. MSSB's systems then should have permitted the user to access data only with respect to those customers whose data the user was properly entitled to view. Finally, MSSB installed and maintained technology controls that, among other things, restricted employees from copying data onto removable storage devices and from accessing certain categories of websites.

8. But MSSB failed to ensure the reasonable design and proper operation of its policies and procedures in safeguarding confidential customer data. In particular, the authorization modules were ineffective in limiting access with respect to one report available

through the FID Select Portal and absent with respect to one of the reports available through the BIS Portal. Moreover, MSSB failed to conduct any auditing or testing of the authorization modules for the Portals at any point since their creation at least 10 years ago. Such auditing or testing would likely have revealed the deficiencies in these modules. Finally, MSSB did not monitor user activity in the Portals to identify any unusual or suspicious patterns.

B. Marsh's Identification and Exploitation of Flaws in the Portals

9. Marsh joined MSSB in April 2008 as a sales assistant. In 2010, Marsh entered MSSB's trainee program and eventually became a CSA based in the New York office. In this role, Marsh supported the work of the FAs in his group. In March 2014, Marsh was promoted to FA. In both his CSA and FA capacities, Marsh ran reports from several applications, including the Portals, that accessed and analyzed confidential customer data.

10. In or about June 2011, while he was employed as a CSA, Marsh discovered that the authorization module for the FID Select Portal did not work when he ran a particular report called the Account Analysis Report. Although the Portal should have restricted Marsh to accessing only customer data associated with the FAs whom he supported, Marsh noticed that he could run this report for all MSSB customers, including those outside his group. A programming flaw in the authorization module for the FID Select Portal caused the module to not interface properly with the employee data entitlements database applicable to that Portal. As a result, a CSA like Marsh was able to access customer data for any FA group throughout MSSB.

11. Marsh repeatedly exploited this programming flaw by first entering a branch ID number other than his own — numbers that were generally available throughout MSSB — and then entering various possible FA or FA group numbers until he discovered a combination that worked. At that point, Marsh was able to and did run reports containing PII of all customers of that FA or FA group. In addition, although Marsh's entitlements to access particular data were supposed to change when he was promoted to FA in March 2014, MSSB failed to make such an entitlements change for the FID Select Portal, the entitlements for which were maintained in a database that was separate from the firm-wide entitlements database. Thus, Marsh continued his unauthorized accessing of confidential customer data until shortly before MSSB discovered his misconduct in late December 2014. From October 2013 through December 2014, Marsh conducted approximately 4,000 unauthorized searches of customer data using the FID Select Portal.[2]

12. By May 2014, Marsh had discovered and, in May 2014, began exploiting a separate and independent deficiency with respect to the BIS Portal — namely, that this portal lacked any authorization module whatsoever for its Relationship Migration Book Analysis Report. Thus, any CSA or FA was able to run this report and gather confidential customer data for other FAs' customers. In 2014, Marsh conducted approximately 1,900 unauthorized searches of customer data in the BIS Portal, using the same approach he used to access the FID Select Portal.

[2] MSSB could not determine the number of Marsh's inappropriate requests prior to October 2013 because it did not retain certain historical data for the period in question.

13. After downloading the data he accessed via the Portals, Marsh transferred the data to a personal server located at his home. MSSB had installed and maintained certain technology controls on its computer systems that, among other things, restricted employees from copying data onto removable storage devices and from accessing certain categories of websites. But Marsh transferred customer data to his personal server by accessing his personal website, galenmarsh.com, which had a feature that enabled Marsh to transfer data from his MSSB computer to his personal server. At the time, MSSB's Internet filtering software did not prevent employees from accessing such "uncategorized" websites from MSSB computers.[3]

C. Data Breach and MSSB's Response

14. Between approximately December 15, 2014 and February 3, 2015, portions of the data downloaded by Marsh were posted to at least three Internet sites, purportedly for sale to a third party. MSSB discovered the data breach through one of its routine Internet sweeps on December 27, 2014. MSSB promptly took steps to remove this data from the Internet and notified law enforcement and other authorities.

15. After comparing certain data reports generated by Marsh to the information posted on the Internet, MSSB identified Marsh as the likely source of the data breach. On December 29 and 30, 2014, MSSB interviewed Marsh, who acknowledged that he had accessed and downloaded confidential customer data to his personal server. Marsh denied posting any of the data on the Internet. Subsequent forensic analysis of Marsh's personal server revealed that a third party likely hacked into the server and copied the confidential customer data that Marsh had downloaded. On January 5, 2015, MSSB began notifying those customers impacted by the data breach.

Violations

16. Adopted pursuant to the Exchange Act and the Advisers Act, among other statutes, the Safeguards Rule requires broker-dealers and investment advisers registered with the Commission to adopt written policies and procedures that address administrative, technical, and physical safeguards reasonably designed to: (1) insure the security and confidentiality of customer records and information; (2) protect against 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.

17. During the relevant period, MSSB maintained customer PII in numerous internal databases accessible by both the BIS Portal and the FID Select Portal. Although MSSB had

[3] Internet filtering programs generally attempt to categorize websites based on their content or other attributes and then apply predetermined filters based on the detected website category. For example, a filtering program may use, among others, such categories as "social media" or "e-commerce." "Uncategorized" websites are those that the filtering program has not placed into one of its established categories.

adopted written policies and procedures relating to the protection of customer PII, those policies and procedures were not reasonably designed to safeguard its customers' PII as required by the Safeguards Rule. For example, MSSB's written policies and procedures failed to adequately address certain key administrative, technical and physical safeguards, such as: reasonably designed and operating authorization modules for the BIS Portal and the FID Select Portal to restrict employee access to only the confidential customer data as to which such employees had a legitimate business need; auditing and/or testing of the effectiveness of such authorization modules; and monitoring and analyzing of employee access to and use of the Portals.

18. As a result of the conduct described above, MSSB willfully[4] violated Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)), which requires every broker-dealer and investment adviser registered with the Commission to adopt written policies and procedures that are reasonably designed to safeguard customer records and information.

Remedial Efforts

19. In determining to accept the Offer, the Commission has considered the remedial efforts promptly undertaken by Respondent and its cooperation afforded to the Commission Staff.

IV.

In view of the foregoing, the Commission deems it appropriate and in the public interest to impose the sanctions agreed to in Respondent's Offer.

Accordingly, pursuant to Sections 15(b) and 21C of the Exchange Act, and Sections 203(e) and 203(k) of the Advisers Act, it is hereby ORDERED that:

A. MSSB cease and desist from committing or causing any violations and any future violations of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)).

B. MSSB is censured.

C. MSSB shall, within ten days of the entry of this Order, pay a civil money penalty in the amount of $1,000,000 to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Exchange Act Section 21F(g)(3). If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. § 3717. Payment must be made in one of the following ways:

[4] A willful violation of the securities laws means merely "'that the person charged with the duty knows what he is doing.'" *Wonsover v. SEC*, 205 F.3d 408, 414 (D.C. Cir. 2000) (quoting *Hughes v. SEC*, 174 F.2d 969, 977 (D.C. Cir. 1949)). There is no requirement that the actor "'also be aware that he is violating one of the Rules or Acts.'" *Id.* (quoting *Gearhart & Otis, Inc. v. SEC*, 348 F.2d 798, 803 (D.C. Cir. 1965)).

(1) MSSB may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;

(2) MSSB may make direct payment from a bank account via Pay.gov through the SEC website at http://www.sec.gov/about/offices/ofm.htm; or

(3) MSSB may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center
Accounts Receivable Branch
HQ Bldg., Room 181, AMZ-341
6500 South MacArthur Boulevard
Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying MSSB as a Respondent in these proceedings and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to Joseph G. Sansone, Co-Chief, Market Abuse Unit, Division of Enforcement, Securities and Exchange Commission, Brookfield Place, 200 Vesey Street, Suite 400, New York, New York 10281.

By the Commission.

Brent J. Fields
Secretary