UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 95832 / September 20, 2022

INVESTMENT ADVISERS ACT OF 1940
Release No. 6138 / September 20, 2022

ADMINISTRATIVE PROCEEDING
File No. 3-21112

In the Matter of **MORGAN STANLEY SMITH BARNEY LLC,** **Respondent.**	**ORDER INSTITUTING ADMINISTRATIVE AND CEASE-AND-DESIST PROCEEDINGS, PURSUANT TO SECTIONS 15b 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 ("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 ("Exchange Act") and Sections 203(e) and 203(k) of the Investment Advisers Act of 1940 ("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 brought 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 15b 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

These proceedings arise out of Respondent's failure to protect its customer records and information, including personal identifying information ("PII"), and properly dispose of consumer report information, in connection with the decommissioning of two data centers in 2016. MSSB contracted with a moving and storage company ("Moving Company") to remove thousands of electronic devices from the data centers and to "remove, destroy, or delete" any data contained on such devices. Moving Company had no experience with, or expertise in, providing such data destruction services. According to the contract with MSSB, Moving Company would work with an e-waste management company ("IT Corp A") to wipe or destroy any data present on the decommissioned devices. However, at some point during the engagement, Moving Company stopped working with IT Corp A and instead began selling unwiped devices removed from MSSB's data centers to another third party ("IT Corp B"). As a result of MSSB's failure to oversee its vendor, Moving Company sold approximately 4,900 information technology assets, including unwiped hard drives, some of which, cumulatively, contained thousands of pieces of PII of MSSB's customers.

In addition, MSSB failed to properly safeguard customer PII and properly dispose of consumer report information on servers decommissioned from various local MSSB offices or branches. In 2019, MSSB decommissioned approximately 500 of these local devices as part of a broader hardware refresh program. When MSSB undertook a cross-check and reconciliation of all of its records to confirm the destruction of these and previously decommissioned local storage devices, MSSB was unable to locate 42 of the devices. The 42 missing devices all potentially contained unencrypted customer PII and consumer report information. The local devices were equipped with encryption capability, but MSSB failed to activate the encryption software until 2018. Once activated, however, due to a manufacturer flaw, the encryption software only encrypted newly created data. As a result of this flaw and MSSB's failure to activate the encryption software until 2018, some data stored on the devices prior to 2018 remained unencrypted.

Respondent

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

[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.

Facts

2016 Data Center Decommissioning

1. MSSB retained Moving Company to decommission its two primary data centers in Poughkeepsie, NY and Columbus, OH ("2016 Data Center Decommissioning). Moving Company handled approximately 4,900 devices, many of which were non-data-bearing devices but some of which contained unencrypted customer PII and consumer report information, including 53 Redundant Array of Independent Disk arrays ("RAID Arrays") that collectively contained approximately 1,000 hard drives. Moving Company also removed approximately 8,000 back-up tapes from one of the data centers.

2. Moving Company and IT Corp A submitted a joint bid in response to MSSB's request for proposal for vendors to handle the planned 2016 Data Center Decommissioning. However, only Moving Company was formally approved as an MSSB vendor. Furthermore, Moving Company was approved as a vendor of data decommissioning services without the use of a sub-vendor. In 2014, MSSB and Moving Company executed a contract for the 2016 Data Center Decommissioning under which Moving Company was retained to pick-up, transport and decommission certain devices from MSSB data centers. That contract also identified IT Corp A and contemplated that the devices from the 2016 Data Center Decommissioning would be wiped (or degaussed) by IT Corp A and resold with 60-70 percent of the resale amount going to MSSB. The contract also contemplated that MSSB would receive an asset report and a disposition report (essentially inventories of the devices collected and whether they were returned to MSSB, resold or destroyed), as well as Certificates of Destruction ("CODs") documenting the destruction of relevant devices.

3. The 2016 Data Center Decommissioning was not conducted in a manner consistent with the terms outlined in the contract. Moving Company collected devices from the data centers and for a brief period delivered those devices to the IT Corp A facility. IT Corp A inventoried devices on its database throughout the collection, wiping and resale process. MSSB had direct access to the database and could have monitored the entire process independently, if it chose to do so. For the devices that it destroyed, IT Corp A provided a COD to Moving Company, which then provided it to MSSB. Devices that were resold were first wiped and then placed for sale on an internet auction site. CODs were not provided for devices that were resold, but wiping was documented in the database. IT Corp A retained a portion of the resale amount (30-40 percent) and provided the remainder of the resale amount to Moving Company. However, it does not appear that MSSB ever requested or received the remainder of the resale amount from Moving Company, as contemplated in the contract. No one at MSSB monitored the database or had any direct contact with IT Corp A during the decommissioning process to ensure that the devices were properly handled.

4. Early in the 2016 Data Center Decommissioning engagement, Moving Company ceased working with IT Corp A. As a result, IT Corp A's inventory tracking database was no longer used. In addition, IT Corp A ceased providing CODs for any devices. This information, which was available to MSSB, indicated that IT Corp A was no longer providing services for the

2016 Data Center Decommissioning.

5. Moving Company then began working with another entity ("IT Corp B") without notifying MSSB. IT Corp B was never vetted by MSSB and was never approved as a vendor or sub-vendor for this decommissioning.

6. Moving Company asked IT Corp B to bid on hard drives that MSSB was selling in an auction. In reality, Moving Company only ever attempted to sell the devices to IT Corp B—there were no other bidders for the devices. IT Corp B had the capability to perform data destruction, but Moving Company never asked IT Corp B to perform those services and IT Corp B understood that the devices had already been wiped. After IT Corp B took possession of the devices from Moving Company, IT Corp B provided Certificates of Indemnification ("COIs"), which simply represented that IT Corp B assumed possession of the devices and risk of loss, and sold the devices to downstream purchasers. Those COIs contained the logo and letterhead of IT Corp B. Moving Company then transmitted the COIs to MSSB via email but referred to them as CODs.

7. MSSB, however, did not review the COIs. If MSSB had reviewed the COIs, it would have been clear that Moving Company was using a sub-vendor that had not been vetted by MSSB and that the hard drives were not being wiped of data, including potential customer PII and consumer report information.

8. Throughout the 2016 Data Center Decommissioning project, Moving Company invoiced MSSB—and was paid—for collecting, shipping, and wiping/degaussing the hard drives, even though no wiping or degaussing services were provided after Moving Company stopped working with IT Corp A.

9. On October 25, 2017, nearly a year after the completion of the 2016 Data Center Decommissioning, MSSB received an email from an IT consultant in Oklahoma ("Consultant"). In that email, Consultant informed MSSB that he had purchased hard drives from an online auction site and that he had access to MSSB's data on those devices. In that email, Consultant informed MSSB that "[y]ou are a major financial institution and should be following some very stringent guidelines on how to deal with retiring hardware. Or at the very least getting some kind of verification of data destruction from the vendors you sell equipment to." MSSB eventually repurchased the hard drives in Consultant's possession.

10. In late 2017, MSSB launched an investigation into the disposition of the devices that were part of the 2016 Data Center Decommissioning project and determined that Moving Company had also delivered the 8,000 back-up tapes removed from one of the data centers to IT Corp B. MSSB emailed IT Corp B on January 19, 2018 asking whether IT Corp B could "confirm the disposition of …3k lbs of tapes." IT Corp B responded: "I can confirm that we did send this load of tapes for secure waste to energy incineration. Although that lot # is not the lot # we used. They were processed 'Confidential Material' in June of 2016." MSSB's basis for believing that these tapes were in fact destroyed without any unauthorized access to customer PII and consumer report information hinges on this email. MSSB has no other verification or

documentation that these tapes were destroyed.

11. In June 2021, MSSB obtained another fourteen of the missing hard drives from a downstream purchaser. Based on forensic analysis of these hard drives, thirteen of the devices contained a total of at least 140,000 pieces of customer PII. The vast majority of the hard drives from the 2016 Data Center Decommissioning remain missing.

12. In July 2020, MSSB provided notice to approximately 15 million impacted customers that "certain devices believed to have been wiped of all information still contained some unencrypted data," including potential PII.

Other Moving Company Projects

13. Between 2015 and 2017, Moving Company was engaged for additional data decommissioning projects for which MSSB did not comply with its internal policies or procedures and/or maintain documentation sufficient to confirm that its policies were followed. For example:

a. In 2015, Moving Company collected approximately 32,000 back-up tapes from MSSB locations in New Jersey and New York and provided them to IT Corp A for shredding. IT Corp A shredded the tapes and provided CODs; however, the destruction of the tapes did not meet the requirements established in MSSBs policies and procedures. MSSB's policies and procedures contain heightened protections for back-up tapes, including a shorter window from removal to destruction, specifications on the devices used to wipe data and sampling to ensure destruction.

b. In 2016, MSSB also retained Moving Company to decommission its New York City data center. MSSB does not have records sufficient to identify the number or types of devices or what data they may have contained. MSSB also does not have CODs for any of those devices.

c. In early 2017, MSSB engaged Moving Company to decommission 61 servers at its Weehawken, New Jersey location, but the employee that hired Moving Company did not go through the required channels for the engagement. In addition, Moving Company provided a COD for the 61 servers, but it did not meet MSSB's standards, which required a COD specifically identifying each of the 244 hard drives that comprised the 61 servers. MSSB requested an updated COD from Moving Company, which was provided, but the serial numbers did not match MSSB's records, raising concerns regarding a possible break in the chain of custody and triggering an internal review. Ultimately, it was determined that the server hard drives bore multiple serial numbers and that MSSB and Moving Company had referred to different serial numbers when they respectively inventoried the drives. Because the devices had already been destroyed, the serial numbers could not be readily reconciled. Ultimately, MSSB was able to validate that the serial numbers identified on Moving Company's COD belonged to MSSB through information obtained from the server and hard drive manufacturers.

d. MSSB has identified an international shipping project that may have involved Moving Company. MSSB can state only that "documents suggest" that Moving Company transported 18-36 unspecified devices to a storage location in New York City. It was contemplated that those devices would be shipped internationally to Europe, potentially by Moving Company. There is no evidence that MSSB actually used Moving Company services in Europe.

WAAS Devices

14. Wide Area Application Services devices ("WAAS" devices) were located at MSSB local branches and stored fragments of data for documents recently accessed by the branch. These devices were intended to shorten the amount of time it took branches to access documents by allowing the branches to by-pass the need to access servers located at the data centers.

15. The WAAS devices were equipped with encryption capability. However, MSSB failed to "turn-on" the encryption capability until 2018. Once the encryption capability was turned on, however, only newly created or overwritten data was encrypted due to a manufacturing flaw in the encryption software. Consequently data that was not overwritten after 2018 remained unencrypted.

16. In 2019, MSSB decommissioned 500 WAAS devices. In February of 2020, MSSB realized that there were four missing WAAS devices ("First WAAS Breach") and also discovered the encryption issue.

17. In 2021, MSSB undertook an inventory of all historical branch devices (including WAAS devices that had been decommissioned prior to 2019) and discovered that an additional 38 devices could not be located ("Second WAAS Breach").

18. MSSB failed to document the final disposition of the WAAS devices, including CODs and documents evincing chain of custody. MSSB also failed to monitor the encryption of data on those branch devices.

19. In July 2020, MSSB provided notice to customers potentially impacted by the First WAAS Breach, and in mid-2021 MSSB provided notice to customers potentially impacted by the Second WAAS Breach.

MSSB's Policies and Procedures Failures

a. Failure to Adopt Written Policies and Procedures

20. MSSB failed to adopt written policies and procedures that identified the high

level of risk associated with the decommissioning of devices. Given that many of MSSB data-bearing devices likely contained PII and consumer report information, and that many of the devices remained unencrypted, all decommissioning projects should have been catalogued as high risk. MSSB's policies and procedures, however, did not require that all such projects be treated as high risk.

21. Although MSSB's contract with Moving Company provided for the resale of decommissioned devices, MSSB did not have written policies and procedures relating to the resale of old or decommissioned devices. The absence of clear policies and procedures relating to the resale of decommissioned devices created confusion that further contributed to the data breach.

b. MSSB's Written Policies and Procedures for Employment and Monitoring of Vendors and Sub-Vendors Were Not Reasonably Designed to Protect the Security and Confidentiality of Customer Records and Information

22. MSSB's written policies and procedures were not reasonably designed because such policies and procedures failed to ensure that a qualified vendor was used for data decommissioning. In fact, Moving Company had no capability to provide the required decommissioning services for the 2016 Data Center Decommissioning. Moving Company is, and has always been, strictly a moving company—a fact that MSSB knew at the time. MSSB, in its September 2, 2013 risk assessment of Moving Company, prior to Moving Company's retention as a vendor, noted that Moving Company provides a variety of services, including "local trucking, storage and long distance moving."

23. In addition, the policies and procedures did not ensure that MSSB reviewed and approved sub-vendors. Although Moving Company represented to MSSB that it was working with IT Corp A to perform the IT decommissioning services, MSSB never conducted a review of IT Corp A or IT Corp B or formally approved either to act as a sub-vendor for the 2016 Data Center Decommissioning. Furthermore, MSSB's policies and procedures were not reasonably designed to ensure that MSSB was aware of a change in the sub-vendor used by Moving Company.

24. MSSB continued to approve Moving Company as a vendor through annual vendor approval documents. In fact, MSSB actually lowered the risk associated with Moving Company between 2015 and 2017. The May 29, 2015 Moving Company vendor approval did not mention any sub-vendor, acknowledged that Moving Company's "security program is not independently assessed leading to potential gaps in security, breaches, and non-compliance with policies and regulatory requirements", and noted that the residual risk associated with Moving Company was "Moderate". The August 1, 2016 Moving Company vendor approval documentation expressly states that there were no material sub-vendors in scope for the assessment, but omitted the fact that Moving Company's security plan had not been independently assessed. That risk assessment again noted that the residual risk associated with Moving Company was "Moderate". Finally, the May 11, 2017 Moving Company risk assessment again noted that there were no material sub-vendors involved and again failed to

note that Moving Company's security plan had not been independently assessed. Furthermore, the risk assessment lowered the residual risk associated with Moving Company to "Low".

25. MSSB's policies and procedures also failed to provide for sufficient monitoring of Moving Company's performance. As early as March 2017, MSSB became aware of problems surrounding Moving Company's maintenance of records. Yet, these problems did not trigger a broader investigation of Moving Company's work for MSSB. In fact, Moving Company continued to work for MSSB throughout 2017. As a result, it wasn't until October 2017 (when Consultant contacted MSSB) that MSSB became aware of the problems surrounding the 2016 Data Center Decommissioning.

26. MSSB's iRespond system requires that personnel "Immediately report suspected or confirmed incidents involving Firm Information being lost, stolen or acquired by an unauthorized party" but did not specifically require that concerns about a vendor be investigated. Reasonably designed policies and procedures would have expressly required that, once MSSB was aware of the problems surrounding the use of Moving Company, a broader investigation of other projects involving Moving Company was initiated.

c. MSSB Failed to Take Reasonable Measures to Protect Customer PII or Consumer Report Information in Connection with Decommissioning Data-Bearing Devices

27. MSSB did not follow its own requirements for documenting the destruction of data, including customer PII or consumer report information, contained on decommissioned devices. MSSB did not obtain CODs, or document the chain of custody for devices throughout the decommissioning process.

28. MSSB failed to implement and monitor compliance with its own policies and procedures relating to the destruction of back-up tapes, which appear to contemplate the significant risk associated with transporting and destroying back-up tapes. Those policies and procedures: (1) specified approved methods for destroying back-up tapes—the preferred method for destruction was shredding followed by incineration; (2) provided a required timeframe for destruction of back-up tapes—24 hours was the maximum amount of time that back-up tapes were permitted to be housed at an approved vendor prior to being destroyed; (3) required that MSSB conduct random sampling of the destroyed tapes; and (4) required that MSSB obtain a COD that specifically outlined the method by which the tapes were destroyed.

29. None of the 40,000 back-up tapes handled by Moving Company complied with these policies and procedures. MSSB never inspected the equipment used to destroy those tapes, the tapes were not destroyed within 24 hours and MSSB never did random sampling. Furthermore, the COD from IT Corp A for 32,000 back-up tapes did not specify the method by which the tapes were destroyed. For the 8,000 tapes delivered to IT Corp B, MSSB never received a COD—in fact MSSB didn't even know that the tapes had been sent to IT Corp B. MSSB received only an email from IT Corp B, 18 months after the fact, stating that the tapes had been destroyed by yet another unapproved sub-vendor.

30. For example, MSSB disregarded its own policies and procedures with respect to the transport and destruction of data bearing devices, including those devices bearing customer PII or consumer report information. The devices at issue each consisted of a controller with multiple hard drives housed in a shelf. When information was sent to the device, the controller spliced the data across the hard drives (in a process known as striping). In order to access data, a majority of the hard drives must be operational and assembled in the correct order. MSSB's policies and procedures acknowledge this aspect of RAID Arrays—they advise that multiple hard drives from a single RAID Array not be transported together or that secure transport methods be used.

31. During the 2016 Data Center Decommissioning, however, MSSB transported hard drive shelves with the drives in place. Witnesses from Moving Company and IT Corp B confirmed that the hard drives were moved from the data centers to IT Corp B's warehouse still in their cabinets, contrary to MSSB's policies and procedures. IT Corp B also sold the shelves to another purchaser with the drives still present.

32. In determining to accept the Offer, the Commission has considered Respondent's remedial efforts.

Violations

33. The Safeguards Rule, Rule 30(a) of Regulation S-P, which the Commission adopted in 2000 pursuant to the Exchange Act and the Advisers Act, among other statutes, and amended in 2005, requires that covered entities, including registered broker-dealers and registered investment advisers, adopt written policies and procedures that address administrative, technical, and physical safeguards reasonably designed for the protection of customer records and information.

34. The Disposal Rule, Rule 30(b) of Regulation S-P, requires that covered entities that maintain or possess consumer report information for a business purpose take reasonable measures to protect against unauthorized access to, or use of, the information in connection with its disposal.

35. MSSB willfully[2] violated the Safeguards Rule because it did not adopt written policies and procedures relating to the safeguarding of customer data, including PII or consumer report information, during the 2016 Data Center Decommissioning and other decommissioning projects.

36. MSSB willfully violated the Disposal Rule because it maintained devices containing consumer report information but failed to take reasonable measures to protect that information during the 2016 Data Center Decommissioning and other decommissioning

[2] "Willfully," for purposes of imposing relief under Section 15(b) of the Exchange Act and Section 203(e) of the Advisers Act, "'means no more than 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." *Tager* v. *SEC*, 344 F.2d 5, 8 (2d Cir. 1965).

projects.

IV.

In view of the foregoing, the Commission deems it appropriate, in the public interest, to impose the sanctions agreed to in Respondent MSSB'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. Respondent MSSB cease and desist from committing or causing any violations and any future violations of Rules 30(a) and (b) of Regulation S-P.

B. Respondent MSSB is censured.

C. Respondent MSSB shall, within 30 days of the entry of this Order, pay a civil money penalty in the amount of $35,000,000 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:

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

(2) Respondent 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) Respondent 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 Celeste A. Chase, Assistant Regional Director, Division of Enforcement, Securities and Exchange Commission, 100 Pearl

Street, Suite 20-100, New York, NY 10004.

D. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondent agrees that in any Related Investor Action, it shall not argue that it is entitled to, nor shall he benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondent's payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondent agrees that it shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondent by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

By the Commission.

Vanessa A. Countryman
Secretary