**STATE OF NEW YORK**
**OFFICE OF THE ATTORNEY GENERAL**

# ASSURANCE OF VOLUNTARY COMPLIANCE[1]

This Assurance of Voluntary Compliance ("Assurance") is entered into by the Attorneys General of Connecticut, Florida, Indiana, New Jersey, New York, and Vermont (the "Attorneys General")[2] and Morgan Stanley Smith Barney LLC ("Morgan Stanley") to resolve the Attorneys General's investigation into two data security incidents reported by Morgan Stanley on or around July 10, 2020. The Attorneys General and Morgan Stanley are collectively referred to as the "Parties".

In consideration of their mutual agreements to the terms of this Assurance, and such other consideration as described herein, the sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

## I. INTRODUCTION AND THE PARTIES

1. This Assurance constitutes a good faith settlement and release between Morgan Stanley and the Attorneys General of claims related to two data security incidents reported by Morgan Stanley on or around July 10, 2020 (collectively referred to herein as the "Data Incidents").

2. The Attorneys General have defined jurisdiction under the laws, or assert jurisdiction under the common law, of their respective States for the enforcement of the Consumer

[1] The term "Assurance" as used herein may refer to an Assurance of Voluntary Compliance or an Assurance of Discontinuance, as applicable.

[2] For ease of reference, this entire group will be referred to collectively herein as the "Attorneys General" or individually as "Attorney General." Such designations, however, as they pertain to Connecticut, shall refer to the Attorney General, both acting on his own behalf and as authorized by the Commissioner of the Department of Consumer Protection. "Connecticut Attorney General" shall mean only the Attorney General. As they pertain to Vermont, shall refer to the Attorney General and Vermont Commissioner of Financial Regulation.

Protection Acts, Personal Information Protection Acts, and Security Breach Notification Acts, as defined below.

3. Morgan Stanley is a limited liability company organized under the laws of Delaware, with its principal place of business headquartered at 1585 Broadway, New York, NY 10036.

## II. COVERED CONDUCT

4. On July 10, 2020, Morgan Stanley notified the Attorneys General of two data security incidents. The first incident involved computer devices that were decommissioned and resold in connection with the closing of two data centers in 2016. While Morgan Stanley had contracted with a vendor to remove its data from the devices, it subsequently learned that the vendor subcontracted certain relevant services to an unauthorized entity, and that certain devices still contained some unencrypted Personal Information (the "Data Center Event"). The second incident involved a software flaw that could have resulted in unencrypted data fragments remaining on the affected devices that Morgan Stanley was unable to locate following a decommissioning event; the data fragments may have remained on the affected devices as a result of a manufacturer flaw in encryption software (the "WAAS Device Event").

5. The Attorneys General began a comprehensive investigation into the Data Center Event and the WAAS Device Event pursuant to the Consumer Protection Acts, Security Breach Notification Acts, and the Personal Information Protection Acts. The investigation determined that Morgan Stanley had failed to maintain adequate vendor controls and hardware inventories, and that had these controls been in place, the Data Incidents could have been prevented.

6. By entering into this Assurance, Morgan Stanley represents that it will maintain appropriate security measures and processes to help prevent these types of incidents from occurring in the future.

## III. DEFINITIONS

For the purposes of this Assurance, the following definitions shall apply:

7. "Consumer" shall mean any individual whose Personal Information Morgan Stanley collects, uses or maintains in connection with providing, or the potential provision of, a product or service to the individual.

8. "Consumer Personal Information" shall mean Personal Information associated with a Consumer.

9. "Consumer Protection Acts" shall mean the state citation(s) listed in Appendix A.

10. "Effective Date" shall be December 9, 2023.

11. "Encrypt" or "Encryption" shall mean the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.

12. "Information System" shall mean a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing Consumer Personal Information or connected to a system containing Consumer Personal Information, as well as a specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains Consumer Personal Information that is connected to a system that contains Consumer Personal Information.

13. "Morgan Stanley" shall mean Morgan Stanley Smith Barney LLC, its affiliates, subsidiaries and divisions, successors and assigns.

14. "Personal Information" or "PI" shall mean: a Social Security number; taxpayer identification number; driver's license number; state identification card number; financial account number; credit or debit card number; passport number; military identification number alien registration number; health insurance identification or policy number; genetic information; medical or health information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; health records of a wellness program or similar program of health promotion or disease prevention; unique biometric data generated from measurements or technical analysis of human body characteristics used to identify or authenticate a consumer; user name, email address, or any other account holder identifying information, in combination with any password, access code, or security question and answer that would permit access to an online account or financial account.

15. "Personal Information Protection Acts" shall mean the State citation(s) listed in Appendix B.

16. "Security Breach Notification Acts" shall mean the State citation(s) listed in Appendix B.

17. "Vendor" shall mean any party that accesses, collects, maintains, disposes of, or otherwise handles data-bearing assets containing Consumer Personal Information on behalf of Morgan Stanley pursuant to a contract with Morgan Stanley.

## IV. APPLICATION

18. The duties, responsibilities, burdens, and obligations undertaken in connection with this Assurance shall apply to Morgan Stanley, its affiliates, subsidiaries, agents, directors,

successors and assigns and its executive management officers having decision-making authority with respect to the subject matter of this Assurance.

## V. GENERAL COMPLIANCE

19. Morgan Stanley shall comply with the Consumer Protection Acts, the Personal Information Protection Acts, and applicable federal law in connection with its collection, use, and maintenance of Consumer Personal Information and shall maintain reasonable security policies and procedures designed to safeguard Consumer Personal Information from unauthorized use or disclosure.

20. Morgan Stanley shall not misrepresent the extent to which it maintains or protects the privacy, security, or confidentiality of Consumer Personal Information.

21. Morgan Stanley shall comply with the reporting and notification requirements set forth in the Security Breach Notification Acts.

## VI. INFORMATION SECURITY PROGRAM

22. Morgan Stanley shall maintain a comprehensive information security program ("Information Security Program") that is reasonably designed to protect the security, confidentiality, and integrity of Personal Information collected directly or indirectly by Morgan Stanley. Morgan Stanley may satisfy the requirement to maintain a comprehensive Information Security Program through the continued development, implementation, review, maintenance, and as necessary, updating of its existing information security program to ensure it meets the requirements set forth in Paragraphs 23 – 42 below.

23. The Information Security Program shall be documented in writing and shall contain administrative, technical, and physical safeguards appropriate to the size and complexity

of Morgan Stanley's operations, the nature and scope of Morgan Stanley's activities, and the sensitivity of the Personal Information that Morgan Stanley maintains.

24. Morgan Stanley shall review its Information Security Program not less than annually and make any updates that are necessary to reasonably protect the privacy, security, and confidentiality of Personal Information that Morgan Stanley collects, stores, and/or transmits, including any updates necessary to minimize the unnecessary retention of such information.

25. Morgan Stanley shall employ an executive or officer responsible for implementing, maintaining, and monitoring the Information Security Program (hereinafter referred to as the Chief Information Security Officer or ("CISO")). The CISO shall have credentials, background, and expertise in information security appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program. Morgan Stanley shall continue to document the duties and responsibilities of the CISO, which include advising senior management of (i) Morgan Stanley's security posture, (ii) security risks faced by Morgan Stanley, including any identified by the Vendor Management Program required under Section IX below, (iii) security events or violations and management's responses thereto, (iv) the security implications of Morgan Stanley's decisions, and (v) recommended changes to the Information Security Program.

26. Morgan Stanley shall provide training on its Information Security Program, including the requirements of this Assurance, to its employees responsible for implementing, maintaining, and monitoring the Information Security Program, including those who report directly or indirectly to the CISO. Morgan Stanley shall provide the training required under this paragraph to such employees on an annual basis, and prior to such employees starting their responsibilities for implementing, maintaining, or monitoring the Information Security Program.

## VII. INCIDENT RESPONSE PLAN

27. Morgan Stanley shall maintain a comprehensive written incident response plan(s).

28. The plan shall require Morgan Stanley to investigate data security incidents that are reasonably suspected to involve Personal Information. Morgan Stanley shall maintain documentation sufficient to show the investigative and responsive actions taken in connection with the incident and the determination as to whether notification is required under the Security Breach Notification Acts. Morgan Stanley shall also assess whether there are reasonably feasible training or technical measures, in addition to those already in place, that would materially decrease the risk of the same type of incident from reoccurring.

29. If Morgan Stanley determines that the incident does not require reporting under the Security Breach Notification Acts, Morgan Stanley shall create a record that includes a description of the incident and Morgan Stanley' response to that event ("Security Event Record").

30. Morgan Stanley shall make the Security Event Record available to the Attorneys General upon request.

## VIII. SPECIFIC SAFEGUARDS

31. **Data Retention & Disposal:** Morgan Stanley shall maintain and comply with policies and procedures governing its collection, use, retention, and disposal of Consumer Personal Information. Such policies and procedures shall require that Consumer Personal Information only be collected, used, and retained consistent with a legitimate business need or legal requirement and securely disposed of when it is no longer needed for such purposes.

A. Morgan Stanley shall comply with a written policy governing the disposal of assets containing Consumer Personal Information in any form (the "Data

Disposal Policy"). This Data Disposal Policy shall be reviewed and updated at least annually, and shall:

(i) Require that Morgan Stanley properly dispose of Consumer Personal Information by taking reasonable measures to protect against unauthorized access to or acquisition of such information, including by shredding, erasing, or otherwise modifying the information to make it unreadable, undecipherable, or otherwise unrecoverable through generally available means; and

(ii) Require that Morgan Stanley continue to perform on-site destruction for all data-bearing assets containing Consumer Personal Information where possible.

32. **Encryption:** Morgan Stanley shall Encrypt Consumer Personal Information at rest and in transit to the extent feasible and consistent with the Firm's annual risk assessments, as described below in paragraph 34. To the extent that Encryption of Consumer Personal Information, either in transit or at rest, is infeasible, Morgan Stanley shall secure such information using reasonable alternative measures that are reviewed and approved in writing by its CISO.

33. **Hardware Inventory:** Morgan Stanley shall employ manual processes and, where practicable, automated tools to regularly inventory, classify, and issue reports on all hardware containing Consumer Personal Information. The inventory shall, where possible, identify the name of the asset, the owner of the asset, the storage location of the asset, and the serial number of the asset. If Morgan Stanley is unable to identify the name of the asset, the owner of the asset, the storage location of the asset, or the serial number of the asset, Morgan Stanley shall document the reason as part of the hardware inventory.

34. **Risk Assessments**: Morgan Stanley shall conduct an annual risk assessment to inform the design of its Information Security Program. Each risk assessment shall be carried out in accordance with written policies and procedures that establish: (1) criteria for the evaluation and categorization of identified security risks or threats faced by Morgan Stanley; (2) criteria for assessment of the confidentiality, integrity, and availability of Morgan Stanley's Information Systems and Consumer Personal Information, including the adequacy of the existing controls in the context of the identified risks faced by Morgan Stanley; and (3) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the Information Security Program will address the risks.

## IX. VENDOR RISK MANAGEMENT PROGRAM

35. Morgan Stanley shall maintain reasonable written policies and procedures to oversee its Vendors' performance of data security and privacy obligations relating to Consumer Personal Information entrusted to such Vendors by Morgan Stanley. Morgan Stanley shall take appropriate steps to confirm that such Vendors are taking reasonable security measures to safeguard such Personal Information.

36. **Vendor Risk Assessment Team:** Morgan Stanley shall maintain a dedicated vendor risk assessment team ("VRA Team") responsible for implementing and maintaining a comprehensive vendor risk management program ("Vendor Management Program"). Members of the VRA Team shall have the appropriate credentials, background, and expertise in information security necessary to effectuate the Program. The VRA Team shall:

A. Maintain reasonable security assessment and monitoring practices to confirm that Vendors are able to comply with Morgan Stanley's security requirements to safeguard Consumer Personal Information, such as Vendor self-assessments

and attestations, third-party audits, formal certifications, risk assessments, penetration tests and/or on-site visits. The frequency, type, and robustness of such assessments and monitoring practices shall be based upon each Vendor's risk rating and consistent with the requirements of this Assurance, provided that Morgan Stanley shall evaluate each Vendor at least once every three (3) years.

B. Conduct written, annual risk assessments for all Vendors involved in the destruction, decommissioning, or disposal of data-bearing assets containing Consumer Personal Information. Such risk assessments shall include financial stability assessments, information security reviews, security architecture assessments, and onsite visits as appropriate based on risk. Once completed, the VRA Team shall submit the assessments for review and approval by the governance committee responsible for overseeing Morgan Stanley asset decommissioning and disposal projects, of which the CISO is a voting member. Members of the governance committee shall have the appropriate credentials, background, and expertise necessary to evaluate Vendor asset decommissioning and disposal risks.

37. **Vendor Management Program Review**: Morgan Stanley shall review the Vendor Management Program not less than annually and make any updates necessary to ensure the reasonable security and confidentiality of Consumer Personal Information that Vendors access, maintain, dispose of, or otherwise handle on behalf of Morgan Stanley.

38. **Vendor Inventory**: Morgan Stanley shall maintain and regularly update an inventory of all active Vendors ("Vendor Inventory") and a copy of active Vendor contracts.

Morgan Stanley shall maintain a risk rating protocol for evaluating its Vendors. In assessing a Vendor's ability to protect and secure Consumer Personal Information, Morgan Stanley shall:

A. Identify the nature and type of Consumer Personal Information that each Vendor may access, maintain, dispose of, or otherwise handle on Morgan Stanley's behalf;

B. Assign a risk rating for each Vendor based on, among other things, the nature and type of Consumer Personal Information accessed, maintained, disposed of, or otherwise handled by each such Vendor; and

C. Record the date(s) of each Vendor's completed risk assessments.

39. **Vendor Contracts - Specific Security Requirements**: In all contracts entered into after the Effective Date of this Assurance, Morgan Stanley shall require Vendors that Morgan Stanley engages to dispose of Consumer Personal Information ("Disposal Vendors") to implement specific data security requirements for protecting Consumer Personal Information, including for the secure disposal of such information.

A. In particular, Morgan Stanley shall contractually require Disposal Vendors to take reasonable measures to securely dispose of such information, including by shredding, erasing, or otherwise modifying the Consumer Personal Information in those records to make it unreadable, undecipherable or otherwise unrecoverable through generally available means. Morgan Stanley shall contractually require Disposal Vendors to appropriately document and provide Morgan Stanley with receipt of its disposal activities.

B. Morgan Stanley shall continue to contractually prohibit Disposal Vendors from reselling or donating hardware containing Consumer Personal Information.

40. Morgan Stanley shall further require that Disposal Vendors agree to flow-down Morgan Stanley's security requirements to subcontractors ("Fourth Parties"), and shall contractually obligate that Disposal Vendors have reasonable policies and procedures in place to monitor Fourth Parties' compliance with such requirements. Any non-compliance with these requirements shall be considered a risk factor in assessing the Disposal Vendor for engagement, including requiring mitigation or remediation of such risk(s) prior to engagement.

41. **Vendor Non-Compliance**: Morgan Stanley shall retain appropriate contractual rights to enforce a Vendor's compliance with Morgan Stanley's security safeguards and policies, which may include notice and cure procedures or termination of the Vendor's contract and/or access to Consumer Personal Information as may be appropriate. Appropriate action includes consideration of the totality of the circumstances, including but not limited to, any failure of the Vendor to perform any of its contractual and legally required security and privacy obligations, the cost and risks involved in terminating such Vendor, and the existence of alternative Vendors to provide the same services.

## X. ASSESSMENT

42. Morgan Stanley represents that it must conduct or obtain assessments of its Vendor Management Program pursuant to independent legal and regulatory requirements. For five (5) years from the Effective Date, Morgan Stanley shall, upon request by the Attorneys General: (1) provide the Attorneys General with an executive summary of any such assessment report, or any provision(s) pertaining to Morgan Stanley's Vendor Management Program in a broader assessment report; and (2) provide the Attorneys General with further information concerning such assessments within thirty (30) days of receiving any requisite permission from Morgan Stanley's regulator(s). Morgan Stanley shall seek such requisite permission within five (5) business days of

receiving a request from the Attorneys General.

## XI. THIRD-PARTY ASSET RECOVERY EFFORT

43. In connection with the resolution of a class action concerning the Data Center and WAAS Device Events, captioned In re Morgan Stanley Data Security Litigation, 1:20-cv-05914-AT (S.D.N.Y) (the "Class Action Settlement"), Morgan Stanley is required to retain a third-party to undertake reasonable efforts to locate and retrieve the remaining assets that were inadvertently sold with Personal Information as part of the Data Center Event. The Parties agree that Morgan Stanley's compliance with this requirement of the Class Action Settlement satisfies compliance with this provision of the Assurance, provided that Morgan Stanley provides to the Attorneys General copies of any reports provided to the United States District Court in connection with the Class Action Settlement concerning these retrieval efforts.

## XII. DOCUMENT RETENTION

44. Morgan Stanley shall retain and maintain all policies, inventories, contracts, and other documentation required by this Assurance for a period of no less than five (5) years from the date of their creation and make them available to the Attorneys General upon request.

## XIII. PAYMENT AND RESTITUTION

45. Within ten (10) business days of the Effective Date, Morgan Stanley shall pay the Attorneys General Six Million Five Hundred Thousand Dollars ($6,500,000.00). Said payment shall be divided and paid by Morgan Stanley directly to each of the Attorneys General in an amount designated by the Attorneys General and communicated to Morgan Stanley by the Indiana Attorney General.

46. Out of the total amount, Morgan Stanley shall pay One Million Six Hundred and Fifty Eight Thousand Forty Seven Dollars and Eighty Cents ($1,658,047.80) to the New York

Attorney General. Said payment shall be used by the New York Attorney General for purposes that may include, but are not limited to, attorney's fees, and other costs of investigation and litigation, or to be placed in, or applied to, any consumer protection law enforcement, consumer education, litigation or local consumer aid fund or revolving fund, used to defray the costs of the inquiry leading hereto, or for other uses permitted by state law, at the sole discretion of the New York Attorney General.

## XIV. GENERAL PROVISIONS

47. The Parties understand and agree that this Assurance shall not be construed as an approval or a sanction by the Attorneys General of Morgan Stanley's business practices, nor shall Morgan Stanley represent that this Assurance is an approval or sanction of its business practices. The Parties further understand and agree that any failure by the Attorneys General to take any action in response to any information submitted pursuant to this Assurance shall not be construed as an approval or sanction of any representations, acts, or practices indicated by such information

48. Nothing in this Assurance should be construed or applied to excuse Morgan Stanley from its obligation to comply with all applicable state and federal laws, regulations, and rules, including its obligation under NY General Business Law § 899-bb to take reasonable measures to protect and secure data in electronic form containing Personal Information.

49. Morgan Stanley shall deliver a copy of this Assurance to, or otherwise fully apprise, its Chief Technology Officer, Chief Information Security Officer, and each member of the governance committee responsible for overseeing Morgan Stanley asset decommissioning and disposal projects within thirty (30) days after the Effective Date.

50. The duties and obligations undertaken in connection with this Assurance shall survive any change in form of doing business or organizational identity and shall apply to Morgan Stanley's successors and assigns, officers, agents, and employees.

51. Morgan Stanley shall not participate in any activity or form a separate entity or corporation for the purpose of engaging in acts or practices, in whole or in part, that are prohibited by this Assurance or for any other purpose that would otherwise circumvent any term of this Assurance. Morgan Stanley shall not knowingly cause, permit, or encourage any other persons or entities acting on its behalf to engage in practices prohibited by this Assurance.

52. As to each individual signatory State, this Assurance shall be governed by the laws of that State without regard to any conflict of laws principles.

53. Facsimile or electronic transmission copies of signatures and notary seals may be accepted as original for the purposes of establishing the existence of this Assurance. This Assurance may be signed in counterparts, which together shall constitute one Assurance.

54. This Assurance is the result of joint negotiations between the Parties and shall be deemed to have been drafted by both the Attorney General and Morgan Stanley. In the event of a dispute concerning the interpretation of this Assurance, the language of this Assurance shall not be construed against either party.

55. Nothing in this Assurance is to be construed as a waiver of any private rights of any person or release of any private rights, causes of action, or remedies of any person against Morgan Stanley or any other person or entity. Nothing herein shall be construed to impair, compromise, or otherwise affect any right of any government agency other than the Attorney General except as expressly limited herein. Nothing herein shall be construed to constitute any express or implied admission of wrongdoing by Morgan Stanley.

56. This Assurance sets forth the entire agreement of the Parties and there are no representations, agreements or understandings between the Parties relating to the subject matter of this Assurance that are not fully expressed herein.

57. If any clause, provision, or section of this Assurance shall, for any reason, be held illegal, invalid, void, or unenforceable, such illegality, invalidity, or unenforceability shall not affect any other clause, provision, or section of this Assurance, and this Assurance shall be construed and enforced as if such illegal, invalid, void, or unenforceable clause, section, or other provision had not been contained herein.

58. The undersigned Morgan Stanley representative(s) state that they are authorized to enter into and execute this Assurance on behalf of Morgan Stanley and further agree to execute and deliver all authorizations, documents, and instruments which are necessary to carry out the terms and conditions of this Assurance.

59. This Assurance may be executed by any number of counterparts and by different signatories on separate counterparts, each of which shall constitute an original counterpart thereof and all of which together shall constitute one and the same document. One or more counterparts of this Assurance may be delivered by facsimile or electronic transmission with the intent that it or they shall constitute an original counterpart thereof.

60. In states where statute requires that this Assurance be filed with and/or approved by a court, Morgan Stanley consents to the filing of this Assurance and to its approval by a court, and authorizes the Attorneys General in such states to represent that Morgan Stanley does not object to the request that the court approve the Assurance. Morgan Stanley further consents to be subject to the jurisdiction of such courts (if legally required) for the exclusive purposes of having such courts approve or enforce this Assurance. To the extent that there are any court costs

associated with the filing of this Assurance (if legally required), Morgan Stanley agrees to pay such costs.

**MORGAN STANLEY SMITH BARNEY LLC**

By: _____

S. Anthony Taggart
(printed name)

Its Managing Director
(title)

Dated this 13th day of November, 2023.

**OFFICE OF THE ATTORNEY GENERAL**
**NEW YORK**

By: /s Clark Russell

Clark P. Russell
Deputy Bureau Chief
Bureau of Internet and Technology
New York State Office of the Attorney General
28 Liberty Street, New York, NY 10005

Dated: 11.16.2023