

ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET & TECHNOLOGY

In the Matter of

Assurance No. 23-014

**Investigation by LETITIA JAMES,
Attorney General of the State of New York, of**

Marymount Manhattan College,

Respondent.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York (“NYAG”) commenced an investigation, pursuant to New York Executive Law § 63(12) and New York General Business Law § 899-bb, into the data security and privacy practices of Marymount Manhattan College (“Respondent” or “MMC”), as a result of a data security incident occurring in or around November 2021 affecting 191,752 actual or prospective students, employees, and alumni, including 99,097 residents of New York. This Assurance of Discontinuance (“Assurance”) contains the findings of the NYAG’s investigation and the relief agreed to by the NYAG and Respondent, whether acting through its respective directors, officers, employees, representatives, agents, affiliates, or subsidiaries (collectively, the “Parties”).

FINDINGS OF NYAG

1. Respondent MMC is a private non-profit liberal arts college located in New York City’s Upper East Side, with its principal building at 221 East 71st Street.
2. To facilitate teaching, administration, and student applications, MMC operated and maintained various computer hardware and software, including servers, databases, computers, files, and applications (“Technical Infrastructure”).

3. MMC routinely collected data from current and prospective students, faculty, and alumni, including social security numbers, bank and credit card numbers, and driver's license numbers. MMC stored that data on its Technical Infrastructure.

4. Sometime before November 12, 2021, a malicious threat actor penetrated MMC's Technical Infrastructure, initially through a Microsoft Exchange Server, gaining access to significant quantities of data concerning 99,097 residents of New York who were actual and prospective students, faculty, and alumni, including social security numbers, dates of birth, bank and credit card numbers, passport numbers, driver's license numbers, medical information, and usernames and passwords (the "breach"). The threat actor then encrypted this information on MMC's servers, and demanded payment in exchange for returning the information.

5. MMC discovered the breach on November 12, 2021. MMC retained an outside IT vendor, incident response counsel, and a digital forensics firm to remediate the incident, conduct an investigation, and to negotiate with the threat actor. MMC paid a ransom for the deletion, non-publication, and return of the data. There is no evidence that any of MMC's data was subsequently made available to any other unauthorized third party.

6. Over the next eight months, MMC investigated the scope of the breach and ultimately provided notice to affected consumers and the NYAG in August 2022 after MMC's data mining vendor concluded its analysis of the exfiltrated files. Some of the data disclosed was over ten (10) years old, and from applicants that never attended the college.

7. After the breach, MMC began to implement new technical and administrative safeguards to protect its Technical Infrastructure, and remediated known vulnerabilities.

MMC's Data Security

8. On August 3, 2022, the NYAG commenced an investigation into the breach and MMC's privacy and data security practices.

9. The NYAG found a number of deficiencies in MMC's technical, administrative, and procedural safeguards for its Technical Infrastructure prior to the breach, including:

a. MMC did not have policies in place to delete student data after a stated retention period, and continued to retain such data indefinitely, for potentially decades.

b. MMC's did not update its existing policies to address new security threats and challenges to its Technical Infrastructure.

c. During the pandemic, MMC suspended its ordinary policies to require users to regularly change their passwords.

d. MMC did not require multi-factor authentication, even for remote access or administrative accounts.

e. MMC did not formalize a patch management process, causing some patches to be delayed and creating vulnerabilities threat actors could exploit.

f. MMC used outdated versions of the Windows operating system with known vulnerabilities to threat actors.

g. MMC did not conduct regular penetration tests.

h. MMC did not engage in regular vulnerability scanning, making it less capable of detecting vulnerabilities when they were present.

i. MMC did not operate a zero trust network, allowing a threat actor to escalate their access after an initial successful attack.

j. MMC did not encrypt sensitive user data at rest or in transit.

Violations of Law

10. By failing to provide reasonable data security, and not providing timely notice, Respondent violated New York Executive Law § 63(12), and New York General Business Law § 899-aa and -bb.

11. By disclosing personally identifiable information from student educational records without consent, Respondent violated 34 C.F.R § 99.30 (“FERPA”).

12. MMC neither admits or denies the NYAG’s Finding, paragraphs 1-11 above.

13. The NYAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the NYAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of Executive Law § 63(12), New York General Business Law § 899-aa and -bb, and 34 C.F.R § 99.30.

IT IS HEARBY UNDERSTOOD AND AGREED, by and between the Parties:

PROSPECTIVE RELIEF

14. MMC shall comply with Executive Law § 63(12), GBL § 899-aa and -bb, FERPA, and the Gramm-Leach-Bliley Act, in connection with its collection, use, disclosure, and maintenance of all social security numbers, financial information, driver’s license numbers, passport numbers, medical information, student information, and health insurance information (“Personal Information”), and shall not misrepresent the manner or extent to which it protects the privacy, security, or confidentiality of Personal Information.

Information Security Program

15. MMC shall maintain, and comply with a comprehensive information security program (“Information Security Program”) that is reasonably designed to protect the security, confidentiality, integrity, and availability of information concerning users on MMC’s Technical Infrastructure. The Information Security Program shall be documented and shall contain administrative, technical, and physical safeguards appropriate to:

- a. The size and complexity of MMC’s operations;
- b. The nature and scope of MMC’s activities; and
- c. The sensitivity of the information concerning users on MMC’s Technical

Infrastructure.

The Information Security Program shall be regularly reviewed and revised not less than annually.

The Information Security Program shall include the requirements of the rest of this Assurance of Discontinuance.

16. MMC shall ensure that employees responsible for implementing, maintaining, or monitoring the Information Security Program receive notice and have sufficient knowledge of the requirements of this Assurance and receive specialized training on safeguarding Personal Information. MMC shall provide the training required under this paragraph to all employees within sixty (60) days of the effective date of this Assurance or within thirty (30) day of when an employee first assumes responsibility for implementing, maintaining, or monitoring the Information Security Program.

17. Once every calendar year, MMC shall provide training on safeguarding Personal Information to its employees who handle such information and its employees responsible for implementing, maintaining, or monitoring the Information Security Program.

18. In addition to the above training requirements, MMC shall also ensure that all employees responsible for building, engineering, developing, or maintaining MMC's Technical Infrastructure receive annual cybersecurity training. MMC shall provide the initial annual training required under this paragraph to all such employees within sixty (60) days of the effective date of this Assurance or within thirty (30) day of when an employee first assumes responsibility for building, engineering, developing, or maintaining MMC's Technical Infrastructure.

Specific Safeguards

19. MMC shall implement appropriate access controls, including without limitation, least privilege access to only allow authorized users access to necessary resources on the MMC network for the organization's business needs, consistent with the principles in NIST Special Publication 800-53 (page 36-39, AC-6), and zero-trust principles, consistent with NIST Special Publication 800-207.

20. MMC shall encrypt all Personal Information on MMCs Technical Infrastructure, when stored and when transmitted, regardless of whether it is stored in a document, database, or elsewhere.

21. MMC shall maintain a reasonable policy to update and patch software on its Technical Infrastructure including the following:

- a. Monitoring software and application security updates and security patch management, including but not limited to receiving notifications from software manufacturers and ensuring the appropriate and timely application of all security updates and/or security patches;
- b. Supervising, evaluating, and coordinating any system patch management

tool(s); and

c. Training requirements for individuals responsible for implementing and maintaining MMC's patch management policies.

22. MMC shall implement and maintain appropriate policies, procedures, and controls to manage access to, and use of, all accounts with access to Personal Information, including, without limitation, administrator accounts. Such policies, procedures, and controls shall be consistent with NIST standards for access control, account management, and digital authentication and at minimum require the following:

a. MMC shall securely store account passwords including hashing passwords stored online using an appropriate hashing algorithm that is not vulnerable to attack, together with an appropriate salting policy, or other equivalent or stronger protections.

b. MMC shall ensure that passwords are not stored in plain text, within any logs or other files. MMC shall ensure that all private encryption keys are stored consistent with parent vendor recommended encryption format.

c. MMC shall require new accounts be given the least access to Personal Information and network resources needed to perform the jobs associated with that account-holder.

d. MMC shall, no less than annually, review accounts with administrative access to ensure that such access is still required to perform the jobs associated with that account-holder.

e. MMC shall maintain account lockout thresholds, such that users who fail to enter a password a number of times in short succession are prohibited from trying again for a period of time.

23. MMC shall enable multifactor authentication for users logging onto MMC's Technical Infrastructure.

24. MMC shall maintain a threat management program that will include the use of automated tools to continuously monitor MMC's Technical Infrastructure for active threats. This shall include tools to identify and block traffic from known malicious IP addresses.

25. MMC shall implement and maintain controls to monitor and log all security and operational activities on MMC's Technical Infrastructure. MMC shall monitor in real time all security and operational activities on MMC's Technical Infrastructure and identify any activity that gives rise to a reasonable likelihood of compromise to the security or confidentiality of Personal Information.

26. MMC shall maintain and monitor, through engagement with a third-party vendor, endpoint detection and response tools on all critical Technical Infrastructure.

27. MMC shall maintain a penetration-testing program reasonably designed to identify, assess, and remediate security vulnerabilities within MMC's Technical Infrastructure. This program shall require penetration testing of MMC's Technical Infrastructure at least once every 12 (twelve) months and promptly, not to exceed thirty (30) days, following any event that requires reporting under New York General Business Law § 899-aa.

28. MMC shall implement and maintain a vulnerability-scanning program reasonable designed to identify, assess, and remediate security vulnerabilities within MMC's Technical Infrastructure. This program shall require scanning of MMC's Technical Infrastructure at least once every 3 (three) months and promptly, not to exceed fifteen (15) days, following any event that requires reporting under New York General Business Law § 899-aa, or any substantial change in MMC's Technical Infrastructure that may create new vulnerabilities, such as changes

in network configuration or new software installation.

29. MMC shall appoint a qualified employee who will be responsible for implementing, maintaining, and monitoring the Information Security Program with the education, qualifications, and experience appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program. The appointed individual shall report directly, at least quarterly, to the President or another individual at MMC with risk-based decision-making authority.

30. MMC shall ensure that the Information Security Program receives the resources and support reasonably necessary to ensure that the Information Security Program functions as required by this Assurance, including a reasonable dedicated budget separate and apart from MMC's information technology ("IT") expenses to provide for appropriate staffing and other security-related expenditures.

Retention Policies

31. MMC shall comply with, and make publicly available on its website(s), a Personal Information retention schedule setting forth: (1) the purpose(s) for which each type of Personal Information is collected; (2) the specific business needs for retaining each type of Personal Information; and (3) a set timeframe for deletion of each type of Personal Information that accounts for any applicable legal or regulatory retention requirements and precludes indefinite retention of such information. MMC shall update the retention schedule as soon as practicable in advance of any changes to it taking effect and inform MMC students, faculty, and alumni of such changes.

Monetary Payment

32. Respondent shall pay to the State of New York One Million Dollars (\$1,000,000) in penalties and costs. The NYAG agrees to suspend the payment subject to the truthfulness, accuracy, and completeness of Respondent's Fiscal Year 2022 through Fiscal Year 2024 financial statements submitted to the NYAG and Respondent's actual and projected budget commitment to spend over \$3.5 million dollars on data security between Fiscal Year 2023 and Fiscal Year 2029. The suspended payment will be immediately due, plus interest computed from the effective date, as per the Rules of Court Procedure of the State of New York, if, upon motion, a court finds that MMC materially deviated from any of these conditions.

Miscellaneous

33. Respondent expressly agrees and acknowledges that the NYAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 40, and agrees and acknowledges that in such event:

- a. any statute of limitations or other time-related defenses are tolled from and after the effective date of this Assurance;
- b. the NYAG may use statements, documents or other materials produced or provided by the Respondent prior to or after the effective date of this Assurance;
- c. any civil action or proceeding shall be adjudicated by the courts of the State of New York, and that Respondent irrevocably and unconditionally waives any objection based upon personal jurisdiction, inconvenient forum, or venue; and
- d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

34. If a court of competent jurisdiction determines that the Respondent has violated the Assurance, the Respondent shall pay to the NYAG the reasonable cost, if any, of obtaining such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

35. This Assurance is not intended for use by any third party in any other proceeding.

36. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of the Respondent. Respondent shall include any such successor, assignment or transfer agreement a provision that binds the successor, assignee or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of the NYAG.

37. Nothing contained herein shall be construed as to deprive any person of any private right under the law.

38. Any failure by the NYAG to insist upon the strict performance by Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the NYAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by the Respondent.

39. All notices, reports, requests, and other communications pursuant to this Assurance shall reference Assurance No. 23-014, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery; express courier; or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to the Respondent, to: Donna Maddux, Partner, or in her absence, to the Chair of the Cybersecurity and Data Privacy Practice Group, Constangy, Brooks, Smith & Prophete, LLP, 4800 SW Meadows Road, Suite 300, Lake Oswego, Oregon 97035. Email correspondence preferred: dmaddux@constangy.com or breachresponse@constangy.com.

If to the NYAG, to: Nathaniel Kosslyn, Assistant Attorney General, or in his absence, to the person holding the title of Bureau Chief, Bureau of Internet & Technology, 28 Liberty Street, New York, NY 10005.

40. The NYAG has agreed to the terms of this Assurance based on, among other things, the representations made to the NYAG by the Respondent and their counsel and the NYAG's own factual investigation as set forth in Findings, paragraphs (1)-(9) above. The Respondent represents and warrants that neither it nor its counsel has made any material representations to the NYAG that are inaccurate or misleading. If any material representations by Respondent or its counsel are later found to be inaccurate or misleading, this Assurance is voidable by the NYAG in its sole discretion.

41. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by the Respondent in agreeing to this Assurance.

42. Respondent represents and warrants, through the signature below, that the terms and conditions of this Assurance are duly approved.

43. The obligations set forth in paragraphs 15-31 shall be implemented within nine (9) months of the effective date of the Assurance, except for paragraph 20, which may be implemented within one (1) year of the effective date of the Assurance.

44. The obligations set forth in paragraphs 15-31 of this Assurance shall expire at the conclusion of the seven (7) year period after the effective date of the Assurance. Nothing in this Agreement shall relieve Respondent of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

45. Respondent agrees not to take any action or to make or permit to be made any public statement denying, directly or indirectly, any finding in the Assurance or creating the impression that the Assurance is without legal or factual basis. Nothing in this paragraph affects Respondent's right to take legal or factual positions in defense of litigation or other legal proceedings to which the NYAG is not a party.

46. Nothing contained herein shall be construed to limit the remedies available to the NYAG in the event that the Respondent violates the Assurance after its effective date.

47. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

48. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of the NYAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.


49. Respondent acknowledges that they have entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

50. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

51. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

52. This Assurance may be executed in multiple counterparts by the parties hereto. All counterparts so executed shall constitute one agreement binding upon all parties, notwithstanding that all parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the effective date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals. Documents executed, scanned and transmitted electronically and electronic signatures shall be deemed original signatures for purposes of this Assurance and all matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

53. The effective date of this Assurance shall be the date of the last signature entered below.

<p>LETITIA JAMES ATTORNEY GENERAL OF THE STATE OF NEW YORK</p> <p>By: <u>Nathaniel Kosslyn</u> Nathaniel Kosslyn Bureau of Internet and Technology Office of the New York State Attorney General 28 Liberty St. New York, NY 10005</p> <p><u>September 20, 2023</u> Date</p>	<p>MARYMOUNT MANHATTAN COLLEGE</p> <p>By: <u></u> Peter Naccarato, Ph. D. Interim President</p> <p>Sep 13, 2023 Date</p>
--	---

Signature:

Email: kjnmarie@mmm.edu

Signature:

Email: wreuter@mmm.edu