

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

In the Matter of

Assurance No. 21-075

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

Wegmans Food Markets, Inc.,

Respondent.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York (“NYAG”) commenced an investigation pursuant to, *inter alia*, Executive Law § 63(12) and General Business Law (“GBL”) §§ 349 and 899-bb into a data security incident (the “Incident”) at Wegmans Food Markets, Inc. (“Wegmans”). This Assurance of Discontinuance (“Assurance”) contains the findings of NYAG’s investigation and the relief agreed to by NYAG and Wegmans.

NYAG FINDINGS

1. On April 5, 2021, a security researcher contacted Wegmans via email regarding a critical security issue. After not receiving a response, the researcher sent a follow-up email on April 12, 2021. Wegmans responded the following day, and the researcher informed Wegmans that a Cloud storage container hosted on Microsoft Azure was left unsecured and open to public access, potentially exposing sensitive information. Wegmans updated the Cloud storage container configurations to prohibit public access.

2. Wegmans then began an investigation of the Incident and confirmed that the

identified storage container had been configured to allow public access. The container had a database backup file with over 3 million records of Customer email addresses and account passwords, the latter of which were hashed and salted. Wegmans concluded the misconfiguration was introduced when the Microsoft Azure container with the database was set up in January 2018.

3. The investigation included a review of the Microsoft Azure environment to identify and address access configuration issues involving other containers. On May 12, 2021, Wegmans identified a second database containing Customers' information that was misconfigured, allowing potential public access to Customers' Personal Information including names, email addresses, mailing addresses, and checksum values derived from driver's license numbers. Wegmans believes the misconfiguration issue was introduced when the Microsoft Azure container with the database was set up in November 2018. Wegmans updated the container configurations to prohibit public access on May 12, 2021.

4. Customers' email addresses and Wegmans account passwords were left potentially exposed for approximately 39 months. The account credentials could have allowed an unauthorized actor to access a Customer's account, or, if the Customer reused their password on other websites, could have been used to access accounts on other websites. The database with Customers' names, email addresses, mailing addresses, and checksum values of their driver's license numbers was left potentially exposed for approximately 30 months.

5. Starting on June 16, 2021, Wegmans began to notify affected Customers of the Incident via substitute notice.

6. The NYAG's investigation identified several areas where Wegmans failed to adopt reasonable data security practices to protect Customers' Personal Information, including:

- a. Access Controls: Wegmans failed to properly configure the access controls of certain Microsoft Azure containers, leaving Customers' Personal Information open to potential public access for over three years. It was only after the Incident that Wegmans implemented practices to ensure proper configuration of access controls during development.
- b. Password Management: At the time of the Incident, the database backup containing Customer email addresses and passwords contained over 1.8 million passwords that were hashed using the SHA-1 hashing algorithm. Given the deficiencies of SHA-1 hashing, Wegmans started transitioning users to the PBKDF2 hashing algorithm to secure passwords in 2016, but nevertheless continued to store passwords with SHA-1 until January 2020. Users who logged in starting in 2016 would automatically have their password hash updated to use the PBKDF2 algorithm. However, if a user had not logged in between 2016 and the date the database backup file was created, their credentials would still have been stored using the SHA-1 format.
- c. Asset Management: Wegmans failed to maintain an asset inventory identifying all Cloud assets containing Personal Information. Accordingly, Wegmans did not conduct security assessments of the subject Cloud databases.
- d. Logging and Monitoring: Wegmans failed to maintain longer-term logging of the Microsoft Azure assets, making it difficult to investigate the Incident. Until recently, Wegmans maintained logs of Azure assets for only 30 days. In addition, Wegmans failed to conduct appropriate security testing of all Cloud

assets.

- e. Data Collection and Retention: The affected information included checksums derived from Customers' driver's license numbers. However, Wegmans did not have a reasonable business purpose for maintaining any form of driver's license information indefinitely. Checksums are not immune from attack and therefore cannot justify the maintenance of unnecessary Personal Information.

7. Wegmans' online privacy policy contains the following representation to consumers:

Securing your personal information is a top priority. We have administrative, technical and physical safeguards in place to protect your information. Our website uses Secure Socket Layer (SSL) encryption so that your personal information cannot be read as it passes over the Internet.

8. Based on the foregoing, Wegmans violated Executive Law § 63(12), and GBL §§ 349 and 899-bb.

9. Wegmans neither admits nor denies NYAG's Findings, paragraphs 1-8 above.

10. 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) and GBL § 899-bb.

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

PROSPECTIVE RELIEF

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

- a. "Customer" shall mean any individual who resides in New York who initiates or completes a purchase of goods or services from Wegmans, or any individual

who resides in New York who otherwise provides Personal Information to Wegmans in connection with Wegmans' website. "Customer" does not include any person who applies for employment through the Wegmans website.

- b. "Cloud" shall mean relating to commercially available shared cloud solutions, such as Microsoft Azure, Amazon Web Services, or Google Cloud.
- c. "Effective Date" shall be the date of the last signature to this Assurance.
- d. "Network" shall mean all networking equipment, databases or data stores, applications, servers, and endpoints that: (1) are capable of using and sharing software, data, and hardware resources; (2) are owned, operated, and/or controlled by Wegmans; and (3) collect, process, store, or have access to Personal Information.
- e. "Personal Information" shall mean information that can be used to identify a Customer, including name, home or other physical address, email address, phone number, account password, Social Security number, government ID number including driver's license number, bank account number, credit or debit card number, or any Private Information.
- f. "Private Information" shall have the same meaning as private information defined in GBL § 899-aa.

GENERAL COMPLIANCE

12. Wegmans shall comply with Executive Law § 63(12), and GBL §§ 349 and 899-bb, in connection with its collection, use, and maintenance of Personal Information, and shall maintain reasonable security policies and procedures designed to safeguard Personal Information

from unauthorized use or disclosure.

13. Wegmans shall not misrepresent the manner or extent to which it maintains and protects the privacy, security, confidentiality, or integrity of Personal Information collected from or about Customers.

INFORMATION SECURITY PROGRAM

14. Wegmans shall maintain a written information security program (“Information Security Program”) that is reasonably designed to protect the security, integrity, and confidentiality of Personal Information that Wegmans collects, stores, transmits, and/or maintains. The Information Security Program shall, at a minimum, include the information security requirements set forth in this Assurance. Wegmans has represented that it maintains such an Information Security Program, and has evaluated, improved upon, and adjusted the Information Security Program in light of the Incident.

15. The Information Security Program shall comply with applicable requirements under New York state law, including General Business Law §§ 899-aa and -bb, and shall contain reasonable administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of Wegmans’ operations; (ii) the nature and scope of Wegmans’ activities; and (iii) the sensitivity of the Personal Information that Wegmans collects, stores, transmits, and/or maintains.

16. Wegmans shall review the Information Security Program not less than annually and make any reasonable changes necessary to ensure the protection of the security, integrity, and confidentiality of Personal Information that Wegmans collects, stores, transmits, and/or maintains.

17. Wegmans shall appoint a qualified employee to be responsible for implementing, maintaining, and monitoring the Information Security Program with the 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. Wegmans has represented that such a qualified employee was in place at the time of the Incident and remains in place. The appointed individual shall report at a minimum semi-annually to the Chief Executive Officer and Board of Directors concerning Wegmans' security posture, the security risks faced by Wegmans, and the Information Security Program.

18. Wegmans shall provide notice of the requirements of this Assurance to its management-level employees responsible for implementing, maintaining, or monitoring the Information Security Program, and shall implement appropriate training of such employees. Wegmans shall provide the training required under this paragraph to such employees within sixty (60) days of the Effective Date of this Assurance or prior to their responsibilities for implementing, maintaining, or monitoring the Information Security Program.

PERSONAL INFORMATION SAFEGUARDS AND CONTROLS

19. Asset Management: Wegmans shall utilize manual processes and, where practicable, automated tool(s) to regularly inventory and classify, and issue internal reports on, all Cloud assets contained within its Network, including but not limited to all software, applications, network components, databases, data stores, tools, technology, and systems. The asset inventory as well as applicable configuration and change management systems shall, at a minimum, collectively identify: (a) the name of the asset; (b) the version of the asset; (c) the owner of the asset; (d) the asset's location within the Network; (e) the asset's criticality rating; (f) whether the asset collects, processes, or stores Personal Information; and (g) each security update and security patch applied or installed during the preceding period.

20. Access Controls: Wegmans shall establish and maintain reasonable policies and procedures to ensure appropriate access controls are in place for all Cloud assets containing Personal Information.

21. Penetration Testing: Wegmans shall implement and maintain a penetration-testing program reasonably designed to identify, assess, and remediate security vulnerabilities within Cloud assets contained within its Network. This program shall include at least one annual comprehensive penetration test of Wegmans' Cloud environment.

22. Logging & Monitoring: Wegmans shall establish and maintain an appropriate system designed to collect and monitor Cloud asset activity, such as through security and event management tools, as well as appropriate policies and procedures designed to properly configure such tools to report anomalous activity. The system shall, at a minimum: (1) provide for centralized logging and monitoring that includes collection and aggregation of logging for Wegmans' Cloud assets, and (2) monitor for and alert security personnel to suspicious activity. Logs for Cloud asset activity should be readily accessible for a period of at least 90 days and stored for at least one year from the date the activity was logged.

23. Customer Password Management: Wegmans shall establish and maintain appropriate password policies and procedures for Customer accounts. Such policies and procedures shall include safeguards to protect stored passwords from unauthorized access, including, without limitation, hashing stored passwords using a hashing algorithm and salting policy at a minimum commensurate with NIST standards and reasonably anticipated security risks. Wegmans shall encourage Customers to use strong passwords and prohibit password reuse. Within eighteen (18) months of the effective date of this Assurance, Wegmans will implement a program

to educate Customers of the benefit of using multifactor authentication for accounts with cards on file and allowing Customers to opt into such use. Wegmans shall periodically review and, where appropriate in light of relevant guidance and reasonably anticipated security risks, update its Customer password requirements.

24. Vulnerability Disclosure: Wegmans shall maintain a reasonable vulnerability disclosure program that allows third parties, such as security researchers, to disclose vulnerabilities to Wegmans. Information regarding the vulnerability disclosure program shall be made conspicuously available on the Wegmans website, including without limitation, in the Wegmans Privacy Policy and/or Terms of Use.

25. Customer Account Controls: Wegmans shall establish and maintain policies and procedures implementing appropriate practices for account management and authentication, including notice, a security challenge, or re-authentication for account changes, such as change of contact information, payment information, or delivery information. Such policies and procedures shall be evaluated on an annual basis.

26. Data Collection: Wegmans shall not collect Personal Information from any Customer without a reasonable business purpose for such collection.

27. Data Deletion: Wegmans shall establish and maintain appropriate policies and procedures to ensure Personal Information is deleted when there is no reasonable business purpose to retain such Personal Information. For Personal Information collected prior to the Effective Date of this Assurance, Wegmans shall permanently delete Private Information for which no reasonable business purpose exists within ninety (90) days of the Effective Date and shall permanently delete all other Personal Information for which no reasonable business purpose exists within two hundred

forty (240) days of the Effective Date.

INFORMATION SECURITY PROGRAM ASSESSMENTS

28. Within one (1) year of the Effective Date, Wegmans shall obtain a comprehensive assessment of the information security of the Cloud assets contained within its Network conducted by a third-party assessor (the “Third-Party Assessment”) which shall be documented (“Third-Party Assessment Report”) and provided to NYAG within fourteen (14) days of completion. Annually for three (3) years thereafter, Wegmans shall obtain Third-Party Assessment Reports which shall be provided to NYAG upon request.

29. The Third-Party Assessment Reports shall, in relation to Wegmans Cloud assets:
- a. Identify the specific administrative, technical, and physical safeguards maintained by Wegmans’ Information Security Program;
 - b. Document the extent to which the identified administrative, technical and physical safeguards are appropriate considering Wegmans’ size and complexity, the nature and scope of Wegmans’ activities, and the sensitivity of the Personal Information maintained on the Network; and
 - c. Assess the extent to which the administrative, technical, and physical safeguards Wegmans has implemented meet the requirements of the Information Security Program.

MONETARY RELIEF

30. Wegmans shall pay to the State of New York Four Hundred Thousand Dollars (\$400,000). Payment shall be made payable to the State of New York in full within thirty (30) days of the Effective Date of this Assurance. Any payment shall reference AOD No. 21-075.

MISCELLANEOUS

31. Wegmans expressly agrees and acknowledges that 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 39, and agrees and acknowledges that in the event the Assurance is voided pursuant to paragraph 39:

- 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 Wegmans prior to or after the Effective Date of this Assurance;
- c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that Wegmans 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).

32. The obligations of this Assurance set forth in Paragraphs 14-27 shall expire at the conclusion of the seven (7) year period after the Effective Date, unless they have expired at an earlier date pursuant to their specific terms. Provided, however, that nothing in this Paragraph shall be construed as excusing or exempting Wegmans from complying with any state or federal law, rule, or regulation.

33. If a court of competent jurisdiction determines that Wegmans has violated the Assurance, Wegmans 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.

34. This Assurance (including without limitation any and all legal and factual statements herein) is not intended to be and shall not in any event be construed or deemed to be, or represented or caused to be represented as, an admission or concession or evidence of any liability or wrongdoing whatsoever on the part of Wegmans or of any fact or violation of any law, rule, or regulation. This Assurance is made without trial or adjudication of any alleged issue of fact or law and without any finding of liability of any kind. This Assurance is not intended for use by any third party in any other proceeding.

35. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of Wegmans. Wegmans shall include in 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 NYAG.

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

37. Any failure by the NYAG to insist upon the strict performance by Wegmans 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 Wegmans.

38. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 21-075, 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 Wegmans, to:

Stephen R. Van Arsdale, Esq.
Senior Vice President, General Counsel & Secretary
Wegmans Food Markets, Inc.
1500 Brooks Avenue
P.O. Box 30844
Rochester, NY 14603-0844

With a copy to:

F. Paul Greene, Esq.
Harter Secrest & Emery LLP
1600 Bausch & Lomb Pl.
Rochester, NY 14604

If to NYAG, to:

Clark Russell, Esq.
Deputy Bureau Chief
(or in his absence, to the person holding the title of Bureau Chief)
Bureau of Internet & Technology
New York State Office of the Attorney General
28 Liberty Street
New York, NY 10005

39. NYAG has agreed to the terms of this Assurance based on, among other things, the representations made to NYAG by Wegmans and its counsel and NYAG's own factual investigation as set forth in NYAG's Findings, paragraphs 1-8 above. Wegmans represents and warrants that neither it nor its counsel has made any material misrepresentations to NYAG. If any material misrepresentations by Wegmans or its counsel are later found to have been made by NYAG, this Assurance is voidable by NYAG in its sole discretion.

40. No representation, inducement, promise, understanding, condition, or warranty not

set forth in this Assurance has been made to or relied upon by Wegmans in agreeing to this Assurance.

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

42. Nothing contained herein shall be construed to limit the remedies available to NYAG in the event that Wegmans violates the Assurance after its Effective Date.

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

44. 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 NYAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

45. Wegmans acknowledges that it has entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

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

47. 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.

48. 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.

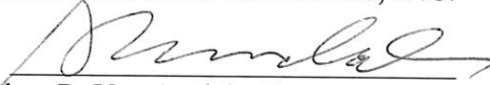
WHEREFORE, THE SIGNATURES EVIDENCING ASSENT TO THIS Assurance have been affixed hereto on the dates set forth below.

LETITIA JAMES
ATTORNEY GENERAL OF THE
STATE OF NEW YORK

By: /s Clark Russell
Clark Russell, Esq.
Deputy Bureau Chief
Jina John, Esq.
Assistant Attorney General
Bureau of Internet and Technology
New York State Office of the Attorney
General
28 Liberty St.
New York, NY 10005

6/21/22
Date

WEGMANS FOOD MARKETS, INC.

By: 
Stephen R. Van Arsdale, Esq.
Senior Vice President, General Counsel &
Secretary
Wegmans Food Markets, Inc.
1500 Brooks Avenue
Rochester, NY 14603

6/2/22
Date