IN THE MATTER OF	*	IN THE CONSUMER PROTECTION
WAWA, INC.	*	DIVISION OF THE OFFICE OF
	*	THE ATTORNEY GENERAL
	*	OF MARYLAND

* * * * * * * * * * * * * *

ASSURANCE OF DISCONTINUANCE

This Assurance of Discontinuance ("Assurance") is entered into by the Attorneys General of Delaware, District of Columbia, Florida, Maryland, New Jersey, Pennsylvania, and Virginia (collectively, the "Attorneys General") and Wawa, Inc. ("Wawa") to resolve the investigation by the Attorneys General into the data security incident announced by Wawa on or about December 19, 2019 (the "Incident").

I. ATTORNEYS GENERAL FINDINGS

1. The Attorneys General allege as follows. Wawa does not admit, agree with, or concede any facts in this Attorneys General Findings sections.

2. Wawa is a privately held company, headquartered in Pennsylvania and incorporated in New Jersey that engages in trade or commerce by owning and operating a chain of more than 850 convenience stores and fuel stations in Delaware, District of Columbia, Florida, Maryland, New Jersey, Pennsylvania, and Virginia under the Wawa name.

3. In connection with the sale of its goods and services, Wawa stores, processes, transmits and receives payment card information ("PCI") from customers to and from the five major credit card brands, including Visa, MasterCard, American Express, Discover, and the Japan Credit Bureau (the "Payment Card Brands").

4. On December 10, 2019, Wawa became aware that there was malware capable of accessing and acquiring payment card information running on payment processing servers at Wawa

stores. This malware was designed to collect customers' payment card data, including card number, expiration date, and cardholder name. It did not collect payment card PIN numbers, credit card CVV2 codes (the three or four digit security codes printed on the back of card) or other PIN numbers. By December 12, 2019, Wawa had blocked this malware. By December 18, 2019, Wawa had deleted the malware completely from its systems.

5. On January 28, 2020, Wawa issued a press release stating that the company learned of reports of criminal attempts to sell cardholder data purportedly related to the Incident. Wawa further stated that it had alerted its payment card processor, the Payment Card Brands, and card issuers to heighten fraud monitoring activities to help further protect any customer information.

6. Approximately thirty-four (34) million payment cards were used at Wawa stores between April 18, 2019 and December 12, 2019, when the malware was running on Wawa's point of sale terminals. The full scope of the compromise and how many of these 34 million cards were involved remains unknown because the malicious actor(s) deleted collected payment card data to avoid detection.

7. In investigating the Incident, the Payment Card Industry Forensic Investigator ("PFI"), claimed that he found three violations of Payment Card Industry Data Security Standards ("PCI DSS").

8. During the Incident, Wawa's Information Security Team ("IS Team") was responsible for reviewing security information events management alerts ("SIEM"); however, this effort did not result in the generation of a log during this particular time period. Wawa, therefore, cannot produce in the form of a specific "log" any alerts from the SIEM received prior to November 2019.

9. The Attorneys General allege that Wawa failed to employ reasonable data security measures.

10. The Attorneys General allege the previously mentioned conduct constitutes violations of states' Consumer Protection Acts and Personal Information Protection Acts.

II. ASSURANCES

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

a. **"Cardholder Data Environment"** ("CDE") means Wawa's personnel, processes, and technologies that store, process, or transmit Payment Card Information of Consumers. The CDE definition also includes system components or devices that are located within or connected to the CDE. This definition is intended to be consistent with the PCI DSS.

b. **"Compensating Controls"** means the definition in PCI DSS Appendix B of "Compensating Controls."

c. **"Consumer"** means any person who initiates a purchase of or purchases goods directly from any Wawa.

d. **"Consumer Protection Acts"** means the statutes listed in Appendix A.

e. **"Effective Date"** will be July 29, 2022.

f. **"Payment Card Information"** ("PCI") means Cardholder Data ("CHD") and Sensitive Authentication Data ("SAD") as defined by the PCI DSS.

g. **"PCI DSS"** means the active and applicable version of the Payment Card Industry Data Security Standard published by Payment Card Industry Security Standards Council.

h. **"Sensitive Personal Information"** means information contained within the CDE of Consumers that is Payment Card Information ("PCI").

i. **"Personal Information Protection Acts"** means the statutes listed in Appendix B.

j. **"Service Provider"** means a business entity that is not a Payment Card Brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of

another entity. This also includes companies that provide services that control or could impact the security of cardholder data.

APPLICATION

12. The duties, responsibilities, burdens, and obligations undertaken in connection with this Assurance apply to Wawa, its affiliates, subsidiaries, successors and assigns, and its officers and employees in the scope of the performance of their job duties.

GENERAL COMPLIANCE

13. Wawa must comply with any applicable provisions of any laws applicable at any given time related to any collection, use or maintenance of customer payment information, including any then-applicable Consumer Protection Acts and Personal Information Protection Acts.

INFORMATION SECURITY PROGRAM

14. Wawa must develop, implement, and maintain a comprehensive information security program to govern the CDE ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of any Sensitive Personal Information Wawa collects, stores, transmits, and/or maintains, and that must, at a minimum include the requirements set forth in this Assurance to the extent appropriate based on Wawa's assessment of relevant risks.

15. The Information Security Program includes the following components:

a. Documented methods and criteria for managing information security risks, including assessment, prioritization, reduction, and acceptance of risks to a reasonable and appropriate level, and achieving the control objectives listed below:

i. The safeguards must not create a likelihood and impact of harm to Consumers or the public interest such that a remedy is needed.

ii. The safeguards may not require Wawa to curtail its proper objectives (e.g., profit, growth, reputation, market competitiveness) or the utility of Wawa's services to Consumers.

iii. The burden imposed on Wawa by the safeguards must be proportionate to the risk the safeguards reduce to Consumers and the public interest.

b. Wawa must continue to conduct comprehensive risk assessments to its CDE or any other network where Wawa stores Sensitive Personal Information at least annually. Within a reasonable period of time after changes to the security of its CDE or any other network where Wawa stores Sensitive Personal Information that may significantly increase risks to Consumers, Wawa will assess the impact of the change. Comprehensive assessments will include intentional and unintentional foreseeable threats to Personal Information that will harm consumers. Risk assessments will be conducted by parties that are competent to model threats that are relevant to Wawa and who may capably estimate risks that are created by those threats.

c. Information Security Program Assessment: At least annually, Wawa must continue to review the effectiveness of Wawa's Information Security Program.

16. Such Information Security Program must be developed and implemented within One Hundred Eighty (180) days after the Effective Date of this Assurance. For any requirements not fully developed and implemented within One Hundred Eighty (180) days after the Effective Date of this Assurance, Wawa must implement interim Compensating Controls to address the identified risks.

17. The Wawa Information Security Program must be written and contain administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of Wawa's operations; (ii) the nature and scope of Wawa's activities; and (iii) the sensitivity of the Sensitive Personal Information that Wawa maintains.

18. Wawa must employ a qualified employee with appropriate credentials, background, and expertise in information security who will be responsible for overseeing Wawa's implementation and maintenance of the Information Security Program. The duties and responsibilities of the qualified employee must be documented and include advising the Chief Executive Officer and the Board of Directors of Wawa's security posture, security risks faced by Wawa and the security implications of Wawa's decisions.

19. Wawa's Information Security Program must include security awareness training to all personnel with key responsibilities for implementation and oversight of the Information Security Program. Wawa's training must ensure that system, database, and network administrators, and persons with privileged access to the CDE are fully informed of the requirements of the Information Security Program relevant to their functions, which may include password policies, secure data handling, secure storage, transmission and disposal of Sensitive Personal Information, and best practices to prevent attackers from obtaining credentials and other sensitive data through malicious downloads and other threats identified by Wawa. Within Ninety (90) days of the Effective Date, Wawa will provide the training required by this Assurance, and thereafter will provide it to relevant personnel on at least an annual basis.

INFORMATION SECURITY SAFEGUARDS

20. As part of the Information Security Program, Wawa must implement reasonable security for Sensitive Personal Information, including:

a. Wawa must reasonably know the actual and intended location and disposition of Sensitive Personal Information. Wawa may achieve this objective through the use of process diagrams and procedures, information classification procedures, data scanning and inventory systems, asset scanning or management systems, or other means.

b. Wawa must take reasonable steps to ensure that only approved software operates within its environment. Wawa may achieve this objective through the commercially available and reasonable anti-virus and anti-malware programs.

c. Wawa must reasonably know the effectiveness of its safeguards against foreseeable threats through vulnerability assessments, penetration tests, or other methods to achieve this objective as required by PCI DSS.

d. Wawa must segment Sensitive Personal Information from people, systems, and networks outside of the CDE by using network segmentation, or other technical, physical, automated, or logical means.

e. Wawa must employ reasonable measures to detect, investigate, contain, respond to, eradicate, and recover from security incidents within reasonable time periods. Wawa will achieve this objective by using log correlation and alerting, file integrity monitoring, data integrity monitoring, SIEM systems, intrusion detection, prevention systems (IDS/IPS), threat management systems, a documented incident response plan, trained personnel, experts, or tools that sufficiently address the risks of harm cause by security incidents.

f. Wawa must implement reasonable controls to ensure that systems in the CDE are accessed by those with appropriate credentials. Wawa may achieve this objective by providing multi-factor authentication, one-time passcodes, location-specific requirements, or other control enhancements.

g. Wawa must implement and maintain an appropriate system designed to collect, manage, and analyze security logs and monitor its CDE. Wawa may achieve this objective by using a central log management system and log harvesting, parsing, alerting to be notified of anomalies or suspicious activity.

21. Wawa must comply with Payment Card Industry Data Security Standards (PCI DSS) with respect to its CDE.

22. Wawa must validate PCI DSS compliance as a Level 1 merchant/service provider for its CDE by engaging a PCI Qualified Security Assessor ("QSA") to conduct an assessment resulting in the delivery of a PCI Report on Compliance ("ROC") and Attestation of Compliance ("AOC").

23. Wawa shall not withhold any internal or external risk assessment reports prepared for or by Wawa if requested by the PCI QSA during the ROC process, unless such assessment is protected by the attorney-client privilege.

24. Wawa must develop and implement risk/vulnerability management policies that comply with PCI DSS 3.2.1 or the required version of PCI DSS.

25. All cardholder data processing will be protected through the use of a commercially available and reasonable encryption, tokenization or other similar solution approved by PCI DSS.

SETTLEMENT COMPLIANCE ASSESSMENT

26. Wawa must obtain an information security compliance assessment and report for the CDE from a third-party professional ("Third-Party Assessor"), using procedures and standards generally accepted in the profession ("Third-Party Assessment"), within one (1) year after the Effective Date of this Assurance, which deadline may be extended by the Attorneys General upon good cause shown by Wawa. The Third-Party Assessment must:

a. Set forth the specific administrative, technical, and physical safeguards maintained by Wawa;

b. Explain the extent to which such safeguards are appropriate in light of Wawa's size and complexity, the nature and scope of Wawa's activities, and the PCI information handled by Wawa;

c. Explain the extent to which the safeguards that have been implemented meet the requirements of the Information Security Program; and

d. Identify Wawa's Qualified Security Assessor for purposes of PCI DSS validation.

e. A ROC meets the requirement for the Third-Party Assessment.

27. Wawa's Third-Party Assessor will be a Certified Information Systems Security Professional ("CISSP") or a Certified Information Systems Auditor ("CISA"), or a similarly qualified person or organization; and have at least five (5) years of experience evaluating the effectiveness of computer systems or information system security.

28. Within thirty (30) days of completion of the Third-Party Assessor's report, Wawa will provide the Third-Party Assessment report to the New Jersey Attorney General's Office.

29. The identification of any deficiencies or recommendations for correction in the Third-Party Assessor's report will not constitute a violation of this Assurance unless Wawa fails to take corrective action within a reasonable time.

III. PAYMENT TO STATES

30. Wawa will pay Eight Million Dollars ($8,000,000.00) to the Attorneys General. Said payment will be divided and paid by Wawa directly to each of the Attorneys General in an amount designated by the Attorneys General and communicated to Wawa by the Pennsylvania Attorney General and New Jersey Attorney General. Payment must be made no later than thirty (30) days after the Effective Date of this Assurance and receipt of such payment instructions by Wawa from the Pennsylvania Attorney General and New Jersey Attorney General, except where state law requires judicial or other approval of the Assurance, payment must be made no later than thirty (30) days after notice from the relevant Attorney General that such final approval for the Assurance has been secured.

The Attorney General of Maryland's portion of the payment is Four Hundred Eighty Three Thousand and Fifty Seven Dollars and 14/100 ($483,057.14).

31. The payments received by the Office of the Attorney General of Maryland may be used at the sole discretion of the Attorney General, for consumer protection purposes, including consumer protection enforcement or consumer education, to defray the costs of the inquiry leading hereto, monitoring and potential enforcement of this Judgment, or may be used for any other public purpose permitted by state law.

IV. RELEASE

32. Following full payment of the amounts due under this Assurance, the Attorneys General will hereby release and discharge Wawa from all civil claims that the Attorneys General could have brought under the Consumer Protection Acts and the Personal Information Protection Acts, or common law claims concerning unfair, deceptive or fraudulent trade practices based on Wawa's conduct related to the Incident. Nothing contained in this paragraph will be construed to limit the ability of the Attorneys General to enforce the obligations that Wawa has under this Assurance. Further, nothing in this Assurance will be construed to create, waive, or limit any private right of action.

V. PRESERVATION OF AUTHORITY

33. Nothing in this Assurance will be construed to limit the authority or ability of the Attorneys General to protect the interests of his/her State or the people of his/her State. This Assurance will not bar the Attorneys General or any other governmental entity from enforcing laws, regulations, or rules against Wawa for conduct subsequent to or otherwise not covered by the Release. Further, nothing in this Assurance will be construed to limit the ability of the Attorneys General to enforce the obligations that Wawa has under this Assurance.

VI. GENERAL PROVISIONS

34. The Parties understand and agree that this Assurance will not be construed as an approval or sanction by the Attorneys General of Wawa's business practices, nor will Wawa represent that this Assurance constitutes 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 information submitted pursuant to this Assurance will not be construed as an approval or sanction of any representations, acts, or practices indicated by such information, nor will it preclude action thereon at a later date.

35. Nothing contained in this Assurance is intended to be and will not in any event be construed or deemed to be, an admission or concession or evidence of any liability or wrongdoing whatsoever on the part of Wawa 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. Wawa enters into this Assurance for settlement purposes only.

36. This Assurance will not be construed or used as a waiver or any limitation of any defense otherwise available to Wawa in any pending or future legal or administrative action or proceeding relating to its conduct prior to the Effective Date of this Assurance or of Wawa's right to defend itself from, or make any arguments in, any individual or class claims or suits relating to the existence, subject matter, or terms of this Assurance. Nothing in this paragraph affects Wawa's (i) testimonial obligations or (ii) right to take legal or factual positions in defense of litigation or other legal proceedings to which the Attorneys General are not a party.

37. This Assurance is not intended for use by any third-party in any other proceeding and is not intended, and should not be construed, as an admission of liability by Wawa.

38. Except for paragraph 13, this Assurance will expire at the conclusion of the five (5) year period after the Effective Date, except as any provisions may have expired at an earlier date

pursuant to their specific terms; provided, however that nothing in this Assurance will be construed as relieving Wawa of the obligation to comply with all state and federal laws, regulations, and rules, nor will any of the provisions of this Assurance be deemed to be permission to engage in any acts or practices prohibited by such laws, regulations, and rules.

39. Wawa must deliver a copy of this Assurance to, or otherwise fully apprise, its Chief Executive Officer, Chief Information Officer, Head of Information Security, and its General Counsel or Senior Legal Officer within ninety (90) days of the Effective Date. Wawa must also provide a copy of this Assurance to each member of its Board of Directors at the next regularly scheduled Board meeting after the Effective Date. Wawa must deliver a copy of this Assurance to, or otherwise fully apprise, any new Chief Executive Officer, Chief Information Officer, Head of Information Security, its General Counsel or Senior Legal Officer within ninety (90) days from which such person assumes the position with Wawa, and to each new member of its Board of Directors at the Board Member's first regularly scheduled Board meeting.

40. To the extent that there are any, Wawa agrees to pay all court costs associated with the filing of this Assurance. No court costs, if any, will be taxed against the Attorneys General.

41. This Assurance may be executed by any number of counterparts and by different signatories on separate counterparts, each of which will constitute an original counterpart thereof and all of which together will 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 will constitute an original counterpart thereof.

42. Wawa agrees that this Assurance does not entitle it to seek or to obtain attorneys' fees as a prevailing party under any statute, regulation, or rule, and Wawa further waives any right to attorneys' fees that may arise under such statute, regulation, or rule.

43. This Assurance will not be construed to waive any claims of Sovereign Immunity the States may have in any action or proceeding.

VII. SEVERABILITY

44. If any clause, provision, or section of this Assurance is held to be illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability will not affect any other clause, provision, or section of this Assurance, which will be construed and enforced as if such illegal, invalid, or unenforceable clause, section, or provision had not been contained herein.

VIII. NOTICE/DELIVERY OF DOCUMENTS

Whenever Wawa provides notice to the Attorney General under this Assurance, that requirement will be satisfied by sending notice to John M. Abel, Assistant Director for Multistate and Special Litigation, 15th Floor, Strawberry Square, Harrisburg, PA 17120. Any notices or other documents sent to Wawa pursuant to this Assurance will be sent to the following address:

Michael Eckhardt
General Counsel
Wawa, Inc.
260 W. Baltimore Pike
Wawa, PA 19063

Copy To:

Gregory T. Parks, Partner
Morgan, Lewis & Bockius LLP
1701 Market Street
Philadelphia, PA 19103-2921

45. All notices or other documents to be provided under this Assurance will be sent by U.S. mail, certified mail return receipt requested, or other nationally recognized courier service that provides for tracking services and identification of the person signing for the notice or document, and will have been deemed to be sent upon mailing. Additionally, any notices or documents to be provided under this Assurance will also be sent by electronic mail if an email address has been provided. Any party may update its address by sending written notice to the other party.

IN WITNESS WHEREOF, this Assurance is executed by the Parties hereto on the dates set forth below:

[Parties' signature pages continued in the following pages]

FOR THE STATE OF MARYLAND

CONSUMER PROTECTION DIVISION
OFFICE OF THE ATTORNEY GENERAL OF MARYLAND

By: _____ Date: _____

Hanna Abrams
Assistant Attorney General
Consumer Protection Division
Office of the Attorney General
200 St. Paul Place, 16th Floor
Baltimore, MD 21202
(410) 576-7296
habrams@oag.state.md.us

FOR WAWA, INC.

By: _____ Date: _____

Michael Eckhardt
General Counsel
260 W. Baltimore Pike
Wawa, PA 19063

Counsel to Respondent, Wawa, Inc.:

By: _____ Date: _____

Gregory T. Parks
Morgan, Lewis & Bockius LLP
1701 Market Street
Philadelphia, PA 19103-2921
(215) 963-5170
gregory.parks@morganlewis.com