# SECURITY BREACH NOTIFICATION FORM

Delaware Department of Justice
Consumer Protection Unit
820 N. French Street
Wilmington, DE 19801
security.breach.notification@state.de.us

| Type of Report |
|---|
| ◉ Initial Breach Report |
| ○ Addendum to Previous Report |

| Entity That Owns or Licenses the Computerized Data Whose Security Was Breached | | | | | |
|---|---|---|---|---|---|
| Name: | Wawa, Inc. | | | | |
| Street Address: | 260 West Baltimore Pike | | | | |
| City: | Wawa | State: | PA | ZIP Code: | 19063 |

| Submitted By | | | | | |
|---|---|---|---|---|---|
| Name: | Gregory T. Parks | Title: | Partner | | |
| Firm (*if different*): | Morgan, Lewis & Bockius LLP | | | | |
| Street Address: | 1701 Market Street | | | | |
| City: | Philadelphia | State: | PA | ZIP Code: | 19103 |
| Telephone: | 215-963-5170 | Email: | gregory.parks@morganlewis.com | | |
| Relationship to Entity That Was Breached: | Outside Counsel | | | | |

## Type of Organization

| | | |
|---|---|---|
| ☐ Charitable/Non-Profit | ☐ Educational | ☐ Financial Services |
| ☐ Government – Delaware | ☐ Government – Outside Delaware | ☐ Healthcare |
| ☐ Insurance | ■ Retail/Merchant | ☐ Utility |
| ☐ Other (please describe): | | |

## Type of Personal Information Involved in the Security Breach

*Delaware resident's first name or first initial and last name, in combination with 1 or more of the following (mark all that apply)*:

| | |
|---|---|
| ☐ Social Security number | ☐ Driver's license number |
| ☐ Federal identification card number | ☐ Passport number |
| ☐ Individual taxpayer ID number | ☐ Biometric data |
| ☐ Deoxyribonucleic (DNA) profile | ☐ Medical history |
| ☐ Medical treatment by a healthcare professional | ☐ Diagnosis of mental/physical condition by healthcare professional |

☐ Health insurance policy number, subscriber ID number, or any other unique identifier used by health insurer to identify person

■ Account number, credit card account number, or debit card number, in combination with any required security code, access code, or password that would permit access to a financial account

☐ Username or email address, in combination with password or security question and answer to access online account

| Number of Persons Affected | |
|---|---|
| Delaware Residents Only | Unknown |
| Total (*including Delaware*) | Unknown |

| Dates | |
|---|---|
| Breach(es) Occurred (*include start/end dates if known*) | Starting different dates after 3/4/2019 and ending on 12/12/20 |
| Breach(es) Discovered | 12/10/2019 |
| Consumers Notified | 12/19/2019 |

| Form of Notice to Affected Persons* | |
|---|---|
| ☐ Written | ☐ Telephonic |
| ☐ Electronic | ■ Substitute Notice |

** Please attach a sample of the notice*

| Was Notification Delayed Because of Law Enforcement Request? | |
|---|---|
| ○ Yes | ◉ No |

## Type of Security Breach (*mark all that apply*)

- ☐ Loss or theft of device or media
- ☐ Internal system breach
- ☐ Insider wrongdoing
- ■ External breach (*hacking, malware, etc.*)
- ☐ Payment card fraud
- ☐ Inadvertent disclosure
- ☐ Improper disposal
- ☐ Other (*please describe*): _____

## Was Information Encrypted?

○ Yes ◉ No

## Was Encryption Key Acquired?

○ Yes ○ No ◉ N/A

## Brief Description of the Security Breach

On December 10, 2019, Wawa's information security team discovered malware running on payment processing systems at potentially all Wawa locations beginning at different points in time after March 4, 2019 and ending on December 12, 2019. Although the dates may vary and some Wawa locations may not have been affected at all, this malware was present on most store systems by approximately April 22, 2019. Wawa's information security team identified this malware on December 10, 2019, and contained it by December 12, 2019. Wawa also immediately initiated an investigation, notified law enforcement and payment card companies, and engaged a leading external forensics firm to support its response efforts. Because of the immediate steps Wawa took to contain this malware, Wawa believes that as of December 12, 2019, this malware no longer poses a risk to customers using payment cards at Wawa.

Based on Wawa's investigation to date, this malware only affected payment card data, including credit and debit card numbers, expiration dates, and cardholder names on payment cards used at potentially all Wawa in-store payment terminals and fuel dispensers beginning at different points in time after March 4, 2019 and ending on December 12, 2019. Most locations were affected as of April 22, 2019, and some locations may not have been affected at all. No other personal information was accessed by this malware. Debit card PIN numbers, credit card CVV2 numbers, other PIN numbers, and driver's license information captured to verify age-restricted purchases were not affected by this malware. The ATM cash machines in Wawa stores were not affected by this incident. At this time, Wawa is not aware of any unauthorized use of any payment card information as a result of this incident.

Wawa continues to take steps to enhance the security of its systems. Wawa has arranged for a dedicated call center to answer customer questions quickly and is offering credit monitoring and identity theft protection without charge through Experian to anyone whose information may have been involved. At this time, Wawa is not able to determine the number of Delaware residents who may be affected by this incident. Further information about what Wawa has done and what it is recommending to potentially impacted customers can be found in the enclosed notice materials that Wawa is posting on its website.

## Location of Breached Information

- ☐ Desktop computer
- ☐ Portable/Laptop computer
- ☐ Smartphone
- ■ Network server
- ☐ Cloud-Based Server
- ☐ Email
- ☐ Other (*please describe*): _____

## Actions Taken in Response to the Security Breach (*mark all that apply*)

- ☐ Added/strengthened data encryption
- ■ Changed password/strengthened password requirements
- ☐ Created/updated formal written information security plan
- ■ Implemented new technical safeguards
- ☐ Improved physical security
- ☐ Revised policies and procedures
- ☐ Sanctioned workforce members involved (incl. termination)
- ■ Trained or retrained workforce members
- ☐ Implemented periodic technical and nontechnical evaluations/risk analyses/penetration tests
- ☐ Revised contracts with business partners, vendors, subcontractors, service providers
- ☐ Changed business partners, vendors, subcontractors, service providers
- ■ Other (*please describe*): See notice.

## Credit Monitoring or Identity Theft Protection Services Offered?

■ Credit monitoring
■ Identity theft protection

| | |
|---|---|
| Duration: | One year |
| Provider: | Experian |
| Briefly describe services: | Credit monitoring, identity restoration, and identity theft insurance |

## Law Enforcement Agency Notified of Security Breach?

◉ Yes
○ No

| | |
|---|---|
| Name of Agency: | Federal Bureau of Investigation |
| Contact Name and Number: | Philadelphia Field Office, 215-418-4000; New York Field Office, 212-384-1000 |
| Report Number (*if applicable*): | |

**Submit Form**

**An Open Letter from Wawa CEO Chris Gheysens to Our Customers**

**December 19, 2019**

**NOTICE OF DATA BREACH**

Dear Wawa Customers,

At Wawa, the people who come through our doors every day are not just customers, you are our friends and neighbors, and nothing is more important than honoring and protecting your trust. Today, I am very sorry to share with you that Wawa has experienced a data security incident. Our information security team discovered malware on Wawa payment processing servers on December 10, 2019, and contained it by December 12, 2019. This malware affected customer payment card information used at potentially all Wawa locations beginning at different points in time after March 4, 2019 and until it was contained. At this time, we believe this malware no longer poses a risk to Wawa customers using payment cards at Wawa, and this malware never posed a risk to our ATM cash machines. I want to reassure you that you will not be responsible for any fraudulent charges on your payment cards related to this incident, as described in the detailed information below. Please review this entire letter carefully to learn about the resources Wawa is providing and the steps you should take now to protect your information.

I apologize deeply to all of you, our friends and neighbors, for this incident. You are my top priority and are critically important to all of the nearly 37,000 associates at Wawa. We take this special relationship with you and the protection of your information very seriously. I can assure you that throughout this process, everyone at Wawa has followed our longstanding values and has worked quickly and diligently to address this issue and inform our customers as quickly as possible.

**What Happened?**

Based on our investigation to date, we understand that at different points in time after March 4, 2019, malware began running on in-store payment processing systems at potentially all Wawa locations. Although the dates may vary and some Wawa locations may not have been affected at all, this malware was present on most store systems by approximately April 22, 2019. Our information security team identified this malware on December 10, 2019, and by December 12, 2019, they had blocked and contained this malware. We also immediately initiated an investigation, notified law enforcement and payment card companies, and engaged a leading external forensics firm to support our response efforts. Because of the immediate steps we took after discovering this malware, we believe that as of December 12, 2019, this malware no longer poses a risk to customers using payment cards at Wawa.

**What Information Was Involved?**

Based on our investigation to date, this malware affected payment card information, including credit and debit card numbers, expiration dates, and cardholder names on payment cards used at potentially all Wawa in-store payment terminals and fuel dispensers beginning at different points in time after March 4, 2019 and ending on December 12, 2019. Most locations were affected as of April 22, 2019, however, some locations may not have been affected at all. No other personal information was accessed by this malware. Debit card PIN numbers, credit card CVV2 numbers (the three or four-digit security code printed on the card), other PIN numbers, and driver's license information used to verify age-restricted purchases were not affected by this malware. If you did not use a payment card at a Wawa in-store payment terminal or fuel dispenser during the relevant time frame, your information was not affected by this malware. At this time, we are not aware of any unauthorized use of any payment card information as a result of this incident. The ATM cash machines in our stores were not involved in this incident.

**What We Are Doing**

As soon as we discovered this malware on December 10, 2019, we took immediate steps to contain it, and by December 12, 2019, we had blocked and contained it. We believe this malware no longer poses a risk to customers using payment cards at Wawa. As indicated above, we engaged a leading external forensics firm to conduct an investigation, which has allowed us to provide the information that we are now able to share in this letter. We are also working with law enforcement to support their ongoing criminal investigation. We continue to take steps to enhance the security of our systems. We have also arranged for a dedicated toll-free call center (1-844-386-9559) to answer customer questions and offer credit monitoring and identity theft protection without charge to anyone whose information may have been involved, which you can sign up for as described below.

**What You Can Do**

Customers whose information may have been involved should consider the following recommendations, all of which are good data security precautions in general:

- Review Your Payment Card Account Statements. We encourage you to remain vigilant by reviewing your payment card account statements. If you believe there is an unauthorized charge on your payment card, please notify the relevant payment card company by calling the number on the back of the card. Under federal law and card company rules, customers who notify their payment card company in a timely manner upon discovering fraudulent charges will not be responsible for those charges.

- Register for Identity Protection Services. We have arranged with Experian to provide potentially impacted customers with one year of identity theft protection and credit monitoring at no charge to you. Information about these services is available at www.wawa.com/alerts/data-security or call toll-free to 1-844-386-9559.

- Order a Credit Report. If you enroll in the Experian service (at the phone number above) we are offering, you will have access to activity on your credit report. In addition, if you are a U.S. resident, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228.

- Review the Reference Guide. The Reference Guide below provides additional resources on the protection of personal information.

**For More Information**

If you have any questions about this issue or enrolling in the credit monitoring services we are offering at no charge to you, please call our dedicated Experian response phone line at 1-844-386-9559. It is open Monday - Friday, between 9:00 am and 9:00 pm Eastern Time, or Saturday and Sunday, between 11:00 am and 8:00 pm Eastern Time, excluding holidays (which include December 24, December 25, December 31, January 1, and January 20).

Along with the nearly 37,000 Wawa associates in all of our communities, we remain dedicated to serving you every day and being worthy of your continued trust.

Sincerely,

Chris Gheysens
CEO

**December 19, 2019**

## REFERENCE GUIDE

In the event that you suspect that you are a victim of identity theft, we encourage you to remain vigilant and consider taking the following steps:

**Order Your Free Credit Report.** To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

**Place a Fraud Alert on Your Credit File:** To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

| | | | |
|---|---|---|---|
| Equifax | P.O. Box 740241<br>Atlanta, Georgia 30374-0241 | 1-800-525-6285 | www.equifax.com |
| Experian | P.O. Box 9532<br>Allen, Texas 75013 | 1-888-397-3742 | www.experian.com |
| TransUnion | Fraud Victim Assistance Division<br>P.O. Box 2000<br>Chester, Pennsylvania 19016 | 1-800-680-7289 | www.transunion.com |

**Place a Security Freeze on Your Credit File.** You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

| | |
|---|---|
| Equifax | P.O. Box 740241www.equifax.com<br>Atlanta, Georgia 30374-0241 |
| Experian | P.O. Box 9554www.experian.com<br>Allen, Texas 75013 |
| TransUnion | Fraud Victim Assistance Divisionwww.transunion.com<br>P.O. Box 2000<br>Chester, Pennsylvania 19016 |

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years
5. Proof of current address, such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

**Contact the U.S. Federal Trade Commission**. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and the Federal Trade Commission ("FTC"). If you believe your identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580

1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

**For Iowa Residents:** State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

**For Maryland Residents:** You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us

**For Massachusetts Residents:** You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

**For New York Residents:** You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
https://ag.ny.gov/internet/resource-center

NYS Department of State's Division of Consumer Protection
(800) 697-1220
https://www.dos.ny.gov/consumerprotection

**For North Carolina Residents:** You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov

**For Oregon Residents:** State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us

**For Rhode Island Residents:** You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services.