



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 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.

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.
- Order a Credit Report. 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.

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