

[To be placed on Wendy's website dedicated to the payment card incident:  
<https://www.wendys.com/notice>]

**Updates Related to Investigation of Unusual Payment Card Activity at Wendy's**

Update as of July 7, 2016

**Statement of Todd Penegor President and CEO, The Wendy's Company**

Dear Valued Customers,

As we have reported over the past several months, unfortunately, some Wendy's restaurants have been the victim of malicious cyber activity targeting customers' payment card information. We sincerely apologize to anyone who has been inconvenienced as a result of these highly sophisticated, criminal cyberattacks. We have conducted a rigorous investigation to understand what has happened and we are committed to protecting our customers and keeping you informed.

Wendy's first reported unusual payment card activity affecting some restaurants in February 2016. In May, we confirmed that we had found evidence of malware being installed on some restaurants' point-of-sale systems, and had worked with our investigator to disable it. On June 9<sup>th</sup>, we reported that we had discovered additional malicious cyber activity involving other restaurants. That malware has also been disabled in all franchisee restaurants where it has been discovered. We believe that both criminal cyberattacks resulted from service providers' remote access credentials being compromised, allowing access – and the ability to deploy malware – to some franchisees' point-of-sale systems.

We have issued the notification below to provide more information to our customers regarding this incident, our response, and the steps you can take to protect yourself. On behalf of affected franchise locations, we are also providing information about specific restaurant locations in the U.S. and Canada that may have been impacted by these attacks, along with support for customers who may have been affected by the malware variants.

We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. To assist you, Wendy's has now arranged to offer one year of complimentary fraud consultation and identity restoration services to all customers who used a payment card at a potentially affected restaurant during the time when the restaurant may have been affected.

If you have any questions or would like more information, you may call a toll-free number, (866) 779-0485, 8:00 am to 5:30 pm CST, Monday through Friday excluding major holidays to receive additional information regarding accessing the fraud consultation and identity restoration services. Any additional information on this incident will continue to be posted here.

In a world where malicious cyberattacks have unfortunately become all too common for merchants, we are committed to doing what is necessary to protect our customers. We will continue to work diligently with our investigative team to apply what we have learned from these incidents and further strengthen our data security measures. Thank you for your continued patience, understanding and support.

## **What Can You Do?**

We recommend that you review the list of potentially affected franchise restaurants (available [here](#)) to identify if you may have been affected by this incident, and if so, call a toll-free number, (866) 779-0485, 8:00 am to 5:30 pm CST, Monday through Friday excluding major holidays to learn more about the fraud consultation and identity restoration services available to you. Additionally, in line with prudent personal financial management, we encourage our customers to be diligent in watching for unauthorized charges on their payment cards and to quickly report suspicious activity to their bank or credit card company. The phone number to call is usually on the back of the credit or debit card.

## **Where Can I Find More Information?**

Customers may call a toll-free number (866) 779-0485, 8:00 am to 5:30 pm CST, Monday through Friday (excluding major holidays) to receive additional information on the incident as well as accessing the fraud consultation and identity restoration services.

## **How do I Know if I was Affected?**

The Wendy's franchisee locations that may have been involved in this incident and the dates during which they may have been affected can be found [here](#). The potentially affected sites are organized by country and state or Canadian province. If you made a purchase using a payment card at one of the listed restaurants during the relevant timeframe, your information may have been affected.

## **Is there Additional Information Related to Wendy's May 11 Investigation Update?**

Wendy's has received the final report from its investigator related to the separate malware discussed in Wendy's May 11 update. That malware targeted similar payment card information, including credit or debit card number, expiration date, cardholder verification value, and service code, but did not target customer names. As noted in Wendy's May 11 update, Wendy's has disabled and eradicated that malware from all of those franchisee locations. The potentially impacted sites related to that malware are located in the United States. A list of those sites, as well as the dates during which those sites may have been affected, are included in the list of potentially impacted franchisee sites that may be found [here](#). Customers who used a payment card at any restaurant location on the list, including those related to the malware discussed during the May 11 update, have access to one year of complimentary fraud consultation and identity restoration services.

## **How do I Access the Fraud Consultation and Identity Restoration Services?**

Wendy's is offering one year of complimentary fraud consultation and identity restoration services to all customers who used a payment card at any potentially impacted franchisee locations during the affected dates for both malware variants. A list of potentially affected restaurants, and relevant timeframes for each location, can be found [here](#). For instructions on how to access your complimentary year of fraud consultation and identity restoration services call a toll-free number (866) 779-0485, 8:00 am to 5:30 pm CST, Monday through Friday (excluding major holidays).

## **What Services am I Being Offered?**

All potentially impacted U.S. and Canadian individuals will receive one year of complimentary fraud consultation and identity restoration services through Kroll. U.S. and Canadian residents will receive the following services:

- **Fraud Consultation** - You have access to consultation with a dedicated licensed investigator at Kroll. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event. You do not need to sign up for these services in order to access them.
- **Identity Restoration** - If you become a victim of identity theft, an experienced licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your investigator can dig deep to uncover all aspects of the identity theft, and then work to resolve it. You do not need to sign up for these services in order to access them.

### **Will I Be Automatically Charged After the 1 Year of Complimentary Fraud Consultation and Identity Restoration Services?**

No, you will not be automatically charged after your 1 year of complimentary services expires. Please note that if a Kroll licensed investigator is assisting you with identity restoration services after the expiration of the 1-year term, Kroll will continue to provide you with identity restoration services for an additional 2 years.

### **Would Wendy's Ever Contact Me Asking for My Personal Financial Information?**

No. Wendy's will not ask you to provide personal financial information in an email or by telephone. You should always be suspicious of any unsolicited communications that ask for your personal financial information or refer you to a web page asking for personal financial information.

### **Can Someone Steal My Identity With A Stolen Credit Card Number?**

Based on discussions with industry experts, compromised credit card information alone generally is not used to open new lines of credit or steal a person's identity. However, it never hurts to check your credit report.

### **What Should I Do if I am Concerned About Identity Theft?**

Based on discussions with industry experts, compromised payment card information alone generally is not used to open new lines of credit or steal a person's identity. However, it is always a good idea to check your credit report regularly. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. In addition, your state may also offer guidance about how you can prevent or respond to identity theft. It is generally recommended that you promptly report instances of identity theft or suspicious activity to local law enforcement, such as your local police or sheriff's department,

your state's attorney general or the Federal Trade Commission. In Canada, you may also report identity theft to the Canadian Anti-Fraud Centre ([www.antifraudcentre-centreantifraude.ca](http://www.antifraudcentre-centreantifraude.ca) or 1-888-495-8501).

*For U.S. Residents:* You may also obtain additional information from the Federal Trade Commission about steps you can take to avoid identity theft (including how to place a fraud alert or a security freeze on your credit account). Contact information for the FTC is as follows:

- **Federal Trade Commission**  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
[www.ftc.gov/bcp/edu/microsites/idtheft](http://www.ftc.gov/bcp/edu/microsites/idtheft)

*For Residents of Maryland:* You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General, whose contact information is as follows:

- **Maryland Attorney General's Office**  
Consumer Protection Division  
200 St. Paul Place 9001  
Baltimore, MD 21202  
1-888-743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

*For Residents of North Carolina:* You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office, whose contact information is as follows:

- **North Carolina Attorney General's Office**  
Consumer Protection Division  
Mail Service Center  
Raleigh, NC 27699  
1-877-566-7226  
<http://www.ncdoj.gov>

*For Residents of California:* You may also obtain information about preventing and avoiding identity theft from the California Attorney General's Office, whose contact information is as follows:

- **California Attorney General's Office**  
California Department of Justice  
Attn: Office of Privacy Protection  
P.O. Box 944255  
Sacramento, CA 94244-2550  
(916) 322-3360; Toll-free in California: (800) 952-5225