July 5, 2016

CONFIDENTIAL
VIA OVERNIGHT DELIVERY

Office of the Attorney General
Consumer Protection and Antitrust
Bureau
33 Capitol Street
Concord, NH 03301

Re: Incident Notice

To the Office of the Attorney General:

My name is Kris Kaffenbarger, Vice President, System Optimization, and I am writing on behalf of Twin Coast Enterprises, Inc. to inform you of an incident that may have involved the personal information of customers that used payment cards at restaurants in New Hampshire. Twin Coast Enterprises, Inc. is part of The Wendy's Company's franchisee system ("Wendy's"), and independently owns and operates one or more restaurants in New Hampshire that may have been impacted by a payment card security incident recently announced by Wendy's ("Potentially Impacted Restaurants"). Wendy's has been working diligently with U.S. law enforcement and leading third-party forensics experts to seek to ensure that its customers are protected.

The ongoing investigation has confirmed that criminals used malware believed to have been effectively deployed on the point-of-sale systems at the Potentially Impacted Restaurants between January 13, 2016 and June 8, 2016. Accordingly, the payment card information of customers that used a payment card at the Potentially Impacted Restaurants during this time may have been put at risk. The payment card information potentially put at risk includes name, credit or debit card number, expiration date, cardholder verification value, and service code. Please note that the cardholder verification value that may have been put at risk is not the three or four digit value that is printed on the back or front of cards.

Wendy's has disabled the malware in all franchisee restaurants where it has been discovered.

Because Wendy's point-of-sale terminals do not capture customer mailing addresses as part of a transaction, Wendy's is not able to determine how many of the customers whose payment card information may have been put at risk are residents of New Hampshire. In addition, Wendy's is also not able to provide the number of unique credit card transactions that occurred during the timeframe of this incident, as it, and Twin Coast Enterprises, Inc., do not currently have that information from Twin Coast Enterprises, Inc.'s payment card processer. Wendy's is providing substitute notification to the potentially impacted customers on behalf of its franchisees. Wendy's is also offering potentially impacted customers complimentary fraud consultation and identity restoration services. A copy of the notification that will be posted on www.wendys.com on July 7, 2016 is attached to this letter.

In accordance with our ongoing security efforts, we continue to review our policies and procedures with respect to cybersecurity and explore the implementation of enhanced controls as necessary and appropriate.

If you have any other questions regarding this incident or if you desire further information or assistance, please email me at Kris.Kaffenbarger@wendys.com so that I can direct you to the appropriate contact at Twin Coast Enterprises, Inc.

Sincerely,

Kris Kaffenbarger
Vice President, System Optimization,
The Wendy's Company

[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 9th, 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.

Sincerely,

Todd Penegor
President and CEO, The Wendy's Company

Information on this situation is included in Wendy's Press Release distributed on July 7, 2016.

Cliquez ici pour la version française.

Notice of Data Breach

FAQs

What Happened?

Wendy's recently reported additional malicious cyber activity involving some franchisee-operated restaurants. The Company believes this criminal cyberattack resulted from a service provider's remote access credentials being compromised, allowing access – and the ability to deploy malware – to some franchisees' POS systems. Soon after detecting the malware, Wendy's identified a method of disabling it and thereafter has disabled the malware in all franchisee restaurants where it has been discovered. The investigation has confirmed that criminals used malware believed to have been effectively deployed on some Wendy's franchisee systems starting in late fall 2015.

What Information Was Involved?

Based on the facts known to Wendy's at this time, the additional malware targeted the following payment card data: cardholder name, credit or debit card number, expiration date, cardholder verification value, and service code. Please note that the cardholder verification value that may have been put at risk is not the three or four digit value that is printed on the back or front of cards, which is sometimes used in online transactions.

What Are We Doing?

Wendy's has worked aggressively with third-party forensic experts and U.S. federal law enforcement on this investigation, which is ongoing. Wendy's has now arranged to offer 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. For a list of potentially affected restaurants, and relevant timeframes for each location, click 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). 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.

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 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

***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

***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

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

- **Iowa Attorney General's Office**
  Director of Consumer Protection Division
  1305 E. Walnut Street
  Des Moines, IA 50319
  (515) 281-5926
  www.iowaattorneygeneral.gov

***For Residents of Oregon*:** State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows:

- **Oregon Department of Justice**
  1162 Court Street NE
  Salem, OR 97301
  http://www.doj.state.or.us

- **Consumer Hotline**:
  - From Salem: (503) 378-4320
  - From Portland (Toll-Free): (503) 229-5576
  - From Elsewhere in Oregon (Toll-Free): 1-(877)-877-9392

For Residents of Massachusetts: You have a right to obtain a police report relating to 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.

How do I Obtain a Copy of My Credit Report?

For U.S. Residents: You may obtain a free credit report, whether or not you suspect any unauthorized activity on your account, online by visiting www.annualcreditreport.com, by calling toll-free at 1-877-322-8228. You may also obtain a free credit report by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to:

- Annual Credit Report Request Service
  P.O. Box 105281
  Atlanta, GA 30348

You may also obtain a copy of your credit report by contacting any one or more of the national consumer reporting agencies listed below. They can also provide you with additional information about fraud alerts and security freezes:

- **Equifax**
  P.O. Box 740241
  Atlanta, GA 30348
  1-800- 685-1111

www.equifax.com

- **Experian**
  P.O. Box 2002
  Allen, TX 75013
  1-888-397-3742
  www.experian.com

- **TransUnion**
  P.O. Box 2000
  Chester, PA 19016
  1-800-916-8800
  www.transunion.com

For Canadian Residents: You may obtain a free copy of your credit report, whether or not you suspect any unauthorized activity on your account from any one or more of the major credit bureaus listed below:

- **Equifax Canada**
  Box 190 Jean Talon Station
  Montreal, Quebec H1S 2Z2
  1-800-465-7166
  www.equifax.ca

- **TransUnion Canada**
  P.O. Box 338, LCD1
  Hamilton, ON L8L 7W2
  1-800-916-8800
  www.transunion.ca

- **TransUnion (Québec Residents)**
  Centre de relations au consommateur
  CP 1433 Succ. St-Martin
  Laval, Québec H7V 3P7
  1-877-713-3393
  www.transunion.ca

Do I Have to Pay for my Credit Report?

For U.S. Residents: You are entitled to a free annual credit report and may obtain that report online by visiting www.annualcreditreport.com or by calling toll-free at 1-877-322-8228. You may also obtain a free credit report by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to:

- Annual Credit Report Request Service
  P.O. Box 105281

Atlanta, GA 30348

For Canadian Residents: You are entitled to a free annual credit report and may obtain a copy of your credit report by contacting any one or more of the major credit bureaus at the contact information listed under How do I Obtain a Copy of My Credit Report? above.

What is a Fraud Alert and How do I Place one on my Credit File?

A fraud alert is a notice placed on your credit file that alerts creditors that you could be a victim of fraud. Fraud alerts are designed to encourage creditors to take additional steps to verify your identity before creating new credit accounts in your name or taking other actions related to your credit, such as increasing credit limits or adding a card to a pre-existing credit or debit card account.

For U.S. Residents: There are three types of fraud alerts that last for varying time-periods: (1) initial fraud alerts, which last for 90 days, (2) extended fraud alerts, which last for 7 years, and (3) for military personnel, active duty alerts, which last for 1 year. To place a fraud alert on your account, contact one of the three major credit reporting agencies:

- **Equifax**
  P.O. Box 740241
  Atlanta, GA 30348
  1-800-525-6285
  www.equifax.com

- **Experian**
  P.O. Box 2002
  Allen, TX 75013
  1-888-397-3742
  www.experian.com

- **TransUnion**
  P.O. Box 2000
  Chester, PA 19016
  1-800-916-8800
  www.transunion.com

For Canadian Residents: To request a fraud alert be placed on your account, you may contact one of the credit bureaus below:

- **Equifax Canada**
  Box 190 Jean Talon Station
  Montreal, Quebec H1S 2Z2
  1-800-465-7166
  www.equifax.ca

- **TransUnion Canada**
  P.O. Box 338, LCD1
  Hamilton, ON L8L 7W2
  1-800-916-8800
  www.transunion.ca

- **TransUnion (Québec Residents)**
  Centre de relations au consommateur
  CP 1433 Succ. St-Martin
  Laval, Québec H7V 3P7
  1-877-713-3393
  www.transunion.ca

Please note that the credit bureaus in Canada typically charge a $5.00 fee to place a fraud alert.

What is a Security Freeze and How do I Place One on my Credit File?

For U.S. Residents: A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit. Please note that placing a security freeze may prevent you from obtaining credit monitoring services.

To place a security freeze on your credit report, you need to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The cost of placing, removing, or temporarily lifting a security freeze varies by state, but generally costs between $5 and $20 for each action at each credit reporting company.

- **Equifax Security Freeze**
  P.O. Box 105788
  Atlanta, GA 30348
  1-800- 685-1111
  www.equifax.com

- **Experian Security Freeze**
  P.O. Box 9554
  Allen, TX 75013
  1-888-397-3742
  www.experian.com

- **TransUnion**
  P.O. Box 2000
  Chester, PA 19016
  1-888-909-8872
  www.transunion.com

Additional Information for Massachusetts Residents: If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

For Canadian Residents: Security Freezes are not offered in Canada.