HUNTON& WILLIAMS

RECEIVED
14 OCT 14 PM 2:24
CONSUMER PROTECTION DIV.

HUNTON & WILLIAMS LLP
200 PARK AVENUE
NEW YORK, NY 10166-0005

TEL 212 • 309 • 1000
FAX 212 • 309 • 1100

LISA J. SOTTO
DIRECT DIAL: 212 • 309 • 1223
EMAIL: lsotto@hunton.com

FILE NO: 82423.000002

October 9, 2014

Director of Consumer Protection
Office of the Attorney General
1305 E. Walnut Street
Des Moines, IA 50319

To Whom It May Concern:

In accordance with Iowa Code §§ 715C.1, 715C.2, I am writing on behalf of International Dairy Queen, Inc. to provide you with notification regarding the nature and circumstances of a recent data security incident.

International Dairy Queen recently learned of possible fraudulent activity on some payment cards that may have been used at certain Dairy Queen locations in the U.S. Upon learning of the issue, the company launched an extensive investigation and retained external forensic experts to help determine the facts. Because nearly all Dairy Queen locations are independently owned and operated, the company worked closely with affected Dairy Queen franchise owners, as well as law enforcement authorities and the payment card brands, to assess the nature and scope of the issue. As a result of the investigation, the company discovered evidence that the systems of some Dairy Queen locations were infected with the widely-reported Backoff malware that is targeting retailers across the country. The investigation revealed that a third-party vendor's compromised account credentials were used to access systems at some Dairy Queen locations.

Based on the investigation, the company believes certain customers' payment card information may have been compromised as a result of this incident. The affected systems contained customers' names, payment card numbers and expiration dates. At this time, the company has no evidence that other customer personal information, such as Social Security numbers, PINs or email addresses, was compromised as a result of this malware infection. The time periods during which the Backoff malware was present on the affected Dairy Queen systems vary by location. Based on the investigation, the company is confident that this malware has been contained.

Attached for your reference is a copy of the substitute notice posted on the company website on October 9, 2014. Also attached is a list of the impacted Dairy Queen locations in Iowa for which the company is providing this notification, along with the relevant time periods of exposure to the malware. The company is not able to determine the number of Iowa residents who might have been impacted by this issue. There were approximately 9,000 payment card

HUNTON& WILLIAMS

transactions during the relevant periods of exposure at the affected Dairy Queen locations in Iowa that are listed in the attached addendum. The company has arranged to provide free identity repair services for one year to customers who used their payment card at one of the impacted Dairy Queen locations during the relevant time period.

If you have any questions, please do not hesitate to contact me.

Very truly yours,

Lisa J. Sotto

Enclosures

List of Impacted Dairy Queen Locations in Iowa and Relevant Time Periods

Location	Start Date	End Date
DQ Grill & Chill Restaurant 2101 Cedar Plaza Drive Muscatine, IA 52761-2201	Tuesday, August 05, 2014	Friday, August 29, 2014
Dairy Queen Brazier 2960 E. 53rd Street Davenport, IA 52807-3011	Tuesday, August 05, 2014	Friday, August 29, 2014
DQ Grill & Chill Restaurant 108 8th Avenue N Clinton, IA 52732-3816	Monday, August 04, 2014	Friday, August 29, 2014
DQ Grill & Chill Restaurant 100 Center Pt Road Hiawatha, IA 52233-1551	Tuesday, August 05, 2014	Monday, September 01, 2014

INTERNATIONAL DAIRY QUEEN, INC.

7505 Metro Boulevard
PO Box 390286
Minneapolis, MN 55439-0286
Telephone: (952) 830-0200

October 9, 2014

Dear DQ and Orange Julius Customers,

International Dairy Queen, Inc. recently learned of a possible malware intrusion that may have affected some payment cards at certain DQ® locations and one Orange Julius® location in the U.S. Upon learning of the issue, we launched an extensive investigation and retained external forensic experts to help determine the facts. Because nearly all DQ and Orange Julius locations are independently owned and operated, we worked closely with affected franchise owners, as well as law enforcement authorities and the payment card brands, to assess the nature and scope of the issue. As a result of our investigation, we discovered evidence that the systems of some DQ locations and one Orange Julius location were infected with the widely-reported Backoff malware that is targeting retailers across the country. The investigation revealed that a third-party vendor's compromised account credentials were used to access systems at those locations.

Based on the investigation, we have established the following:

- The Backoff malware was present on systems at a small percentage of locations in the U.S.
- The time periods during which the Backoff malware was present on the affected systems vary by location. A list of impacted DQ locations and the one Orange Julius location, as well as the relevant time periods, is available here.
- The affected systems contained customers' names, payment card numbers and expiration dates. We have no evidence that other customer personal information, such as Social Security numbers, PINs or email addresses, were compromised as a result of this malware infection.
- Based on our investigation, we are confident that this malware has been contained.

We deeply regret any inconvenience this incident may cause. Our customers are our top priority and we are committed to working with our franchise owners to address the issue.

We are notifying DQ and Orange Julius customers about this incident so they can take steps to help protect their information. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports. If you believe your payment card may have been affected, contact your bank or payment card issuer immediately. Additional information and security tips are available here.

We are offering free identity repair services for one year to customers in the U.S. who used their payment card at one of the impacted locations during the relevant time period. Information on these services and eligibility can be found here.

If you have any questions about this issue, please call us toll-free at 1-855-865-4456, Monday through Saturday from 8 a.m. CT to 8 p.m. CT.

We sincerely apologize for any inconvenience this may have caused you.

Sincerely,

John Gainor

John Gainor
President and Chief Executive Officer

DATA SECURITY INCIDENT

ADDITIONAL INFORMATION

We encourage affected customers to take 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 ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form. When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Identity Repair Services. We are offering affected customers in the U.S. who used their payment card at one of the impacted Dairy Queen locations or the one impacted Orange Julius location during the relevant time period identity repair services (AllClear SECURE) from AllClear ID for one year at no cost to them. These services start on October 9, 2014 and will be available at any time during the next 12 months. These services provide affected customers with a dedicated investigator to assist them with fraud-related issues arising from this incident. These services are automatically available to affected customers and no enrollment is required. Affected customers may receive these fraud assistance services by calling 1-855-865-4456.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these 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 contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing 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 the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from $5-$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* For more information on security freezes, you may contact the three

nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze. The consumer reporting agencies may charge you a fee of up to $5 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

DATA SECURITY INCIDENT

PRESS RELEASE

MEDIA CONTACT:

Dean A. Peters
Associate Vice President of Communications | American Dairy Queen Corporation
7505 Metro Blvd. | Minneapolis, MN 55439-0286
(952) 830-0204. | dean.peters@idq.com

FOR IMMEDIATE RELEASE
October 9, 2014

INTERNATIONAL DAIRY QUEEN CONFIRMS MALWARE INTRUSION AT SOME U.S. LOCATIONS

EDINA, MINN. — International Dairy Queen, Inc. today confirmed that the systems of some DQ® locations and one Orange Julius® location in the U.S. had been infected with the widely-reported Backoff malware that is targeting retailers across the country. The company previously indicated that it was investigating a possible malware intrusion that may have affected some payment cards used at certain DQ locations in the U.S. Upon learning of the issue, the company conducted an extensive investigation and retained external forensic experts to help determine the facts. Because nearly all DQ and Orange Julius locations are independently owned and operated, the company worked closely with affected franchise owners, as well as law enforcement authorities and the payment card brands, to assess the nature and scope of the issue. The investigation revealed that a third-party vendor's compromised account credentials were used to access systems at some locations.

The investigation has established the following:

- The Backoff malware only impacted payment card data at 395 of the more than 4,500 U.S. locations.
- The time periods during which the Backoff malware was present on the relevant systems vary by location. A list of impacted locations, as well as the relevant time periods, is available at www.dq.com/datasecurityincident/.
- The affected systems contained payment card customer names, numbers and expiration dates. The company has no evidence that other customer personal information, such as Social Security numbers, PINs or email

addresses, was compromised as a result of this malware infection.

- Based on our investigation, we are confident that this malware has been contained.

"*We are committed to working with and supporting our affected DQ and Orange Julius franchise owners to address this incident," said John Gainor, president and CEO of International Dairy Queen. "Our customers continue to be our top priority.*" The company is offering free identity repair services for one year to customers in the U.S. who used their payment card at one of the impacted DQ locations or the one Orange Julius location during the relevant time period. The company has posted information about these services and other steps that affected DQ and Orange Julius customers can take to help protect themselves on the company's website at www.dq.com/datasecurityincident/.

About International Dairy Queen, Inc.

International Dairy Queen, Inc. is the parent company of American Dairy Queen Corporation (ADQ) and Orange Julius of America, which are headquartered in Minneapolis, Minn., and which develop, license and service a system of more than 6,300 Dairy Queen® and Orange Julius® stores in the United States, Canada and 25 other countries. For more information, visit DairyQueen.com.