



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

July 21, 2020

Bruce A. Radke
312-463-6211
312-819-1910 Direct Fax
bradke@polsinelli.com

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)

The Honorable Gordon MacDonald
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of a Data Security Incident

Dear Attorney General MacDonald:

We represent U.S. Restaurants, Inc. (“USRI”) in connection with a recent incident that may have impacted the personal information of twelve (12) New Hampshire residents. USRI is reporting the incident pursuant to N.H. REV. STAT. ANN. § 359-C:20. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While USRI is notifying you of this incident, USRI does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire on personal jurisdiction.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

USRI has learned that, on February 7, 2020, an unauthorized third party accessed a number of USRI’s computer systems without authorization and infected those systems with ransomware. Upon learning of the situation, USRI promptly launched an internal investigation and secured its computer systems to prevent potential further access. USRI also retained a leading forensic security firm to investigate the incident and confirm the security of its computer systems.

After identifying the scope of the incident, USRI worked with a document review vendor to conduct a programmatic review of the contents of the impacted accounts, and then manually review the items identified as potentially at risk by that programmatic review. Due to the scope of the incident and the amount of data involved, this process took a considerable amount of time. On June 15, 2020, USRI determined the identity of the impacted individuals and worked to identify addresses for those individuals and update the addresses based on the National Change of Address database. This research resulted in USRI determining that the impacted systems contained the

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Nashville New York Phoenix
St. Louis San Francisco Seattle Washington, D.C. Wilmington
Polsinelli PC, Polsinelli LLP in California



The Honorable Gordon MacDonald
Office of the Attorney General
July 21, 2020
Page 2

personal information of twelve (12) New Hampshire residents. The impacted information included individuals' names and Social Security numbers.

At this point, USRI is not aware of any fraud or identity theft to any individual as a result of this incident, and cannot confirm if any personal information was actually obtained by an unauthorized person. Nevertheless, because certain computer systems were accessed by the unauthorized third party, and USRI cannot determine exactly what, if any, information may have been obtained, USRI is notifying individuals whose personal information could have been accessed.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

USRI has identified twelve (12) New Hampshire residents whose information may have been accessed by the unauthorized third party. USRI started mailing notification letters to these individuals on July 21, 2020. Included in the notification was information on ways the individuals can protect themselves against potential fraud and identity theft, as well as a telephone number they can call if they have any questions regarding the incident. Individuals also received an offer for a complimentary one-year membership for Experian IdentityWorks 3B credit monitoring and identity theft services. Enclosed is a sample of the notice that is being sent to the impacted individuals via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, USRI promptly contained the incident by securing its computer systems and network to prevent further access. It also engaged a forensic security firm to investigate and confirm the security of its computer systems and network. USRI implemented and is currently undertaking additional efforts to reduce the risk of a similar incident occurring in the future, including updating its administrative, physical, and technical security measures. Finally, as discussed above, USRI is notifying impacted individuals and providing them with information on how they can protect themselves against fraudulent activity and identity theft.

CONTACT INFORMATION

Please do not hesitate contact me if you have any questions or if I can provide you with any further information concerning this matter.



The Honorable Gordon MacDonald
Office of the Attorney General
July 21, 2020
Page 3

Very truly yours,

A handwritten signature in black ink, appearing to read "Bruce A. Radke".

Bruce A. Radke

Enclosure



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

U.S. Restaurants, Inc. (“USRI”) is committed to the privacy of its employees and takes the protection of personal information that is entrusted to us seriously. Although we have no reason to believe that your information has been misused to commit fraud or identity theft, we are writing to make you aware of a recent data security incident that may have involved some of your personal information.

We recently discovered that certain of our computer systems were the target of a cyberattack. Upon learning of the situation, we promptly launched an internal investigation and secured our systems to prevent potential further access. We also retained a leading forensic security firm to investigate the incident and confirm the security of our affected computer systems. After a thorough review of the affected computer systems, on June 15, 2020, we determined that certain files on our systems were subject to unauthorized access and contained your name and Social Security number.

Again, although we are not aware of any instances of fraud or identity theft, we are offering a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

We take our responsibility to safeguard your personal information seriously and apologize for any inconvenience or concern this incident might cause. **For further information and assistance, please call 1-844-952-2224 from 8:00 a.m. to 5:30 p.m. Central Time, Monday-Friday.**

Sincerely,

US Restaurants, Inc.

Michael J. Kadelski
Chief Financial Officer

ACTIVATING YOUR COMPLIMENTARY CREDIT MONITORING

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<b2b_text_1 (Date)>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: <<Member ID>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332. Be prepared to provide engagement number <<b2b_text_2 (Engagement #)>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit>
or call 877-890-9332 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-890-9332.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

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

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-800-349-9960
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

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

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfc_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Iowa Residents: Iowa residents can contact the Office of the Attorney General to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, (515) 281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 220 St. Paul Place, Baltimore, MD 21202, (888) 743-0023.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

Rhode Island Residents: We believe that this incident affected eight (8) Rhode Island residents. Rhode Island residents can contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400.