



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

MAY 04 2018

CONSUMER PROTECTION

Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

April 30, 2018

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent the National Restaurant Association (“the Association”), 2055 L Street NW, Suite 700, Washington, DC 20036, and are writing to notify your office of an incident that may affect the security of personal information relating to five (5) New Hampshire residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, the Association does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

On October 2, 2017, the Association identified a large volume of suspicious emails that appeared to come from an employee email account. The Association immediately launched an internal investigation into the suspicious activity, and worked with leading third-party forensic investigators to confirm the nature and scope of the incident. Through this investigation, the Association learned on or around November 28, 2017, that several employee email accounts were subject to unauthorized logins by an unknown actor. Unfortunately, the investigation was unable to determine whether the unknown actor viewed any specific emails or attachments in the accounts. The emails were reviewed to identify the information in them and the entities to whom the information contained may relate. Through this review, it was determined on January 24, 2018 that personal information relating to a select group of individuals may have been impacted. Since that time, the Association has been diligently working to identify the individuals who may have been impacted and confirm the address information related to same.

The investigation in this matter confirmed that the following types of information related to Association employees, clients, and/or other individuals may have been accessed by the unauthorized actor: name, Social Security number, if contained in the compromised email accounts.

Notice to New Hampshire Residents

On April 30, 2018 the Association began providing written notice of this incident to all affected individuals, which includes five (5) New Hampshire residents. Written notice will be provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

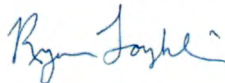
Upon discovering the unauthorized access to personal information, the Association moved quickly to identify those that may be affected, to put in place resources to assist them, and to provide them with notice of this incident. The Association is also reviewing its existing policies and procedures, and working to implement additional safeguards to protect the security of information in its systems.

The Association is providing potentially affected individuals access to one (1) free year of credit monitoring and identity restoration services through TransUnion, and has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, the Association is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. The Association is also providing written notice of this incident to other state regulators and major consumer reporting agencies as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4786.

Very truly yours,



Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/
Enclosure

Exhibit A



Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of a Data Breach

Dear <<Name1>>:

The National Restaurant Association recently discovered an event that might affect the security of your personal information. We are writing to provide you with information about the incident, steps we are taking in response and how you can better protect yourself against the possibility of identity theft and fraud, should you feel it is appropriate.

What Happened: On October 2, 2017, we identified a large volume of suspicious emails that appeared to come from an employee email account. We immediately began to investigate this activity, and worked with leading third-party forensic investigators to learn more about the nature and scope of the incident. Through this investigation, we learned on or around November 28, 2017, that several employee email accounts were subject to unauthorized logins by an unknown actor. Unfortunately, we were not able to determine whether or not the unknown actor viewed specific emails and/or attachments. The emails in the accounts were reviewed to identify the information in them and the individuals to whom the information may relate. Through this review, we determined on Jan. 24, 2018 that your personal information may have been impacted. Since that time, we have been diligently working to identify the individuals who may have been impacted by this event and confirm the address information related to same.

<<Data Elements Paragraph>>

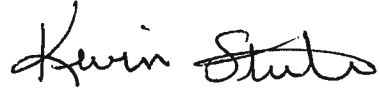
What We Are Doing: We take this incident and the security of your personal information seriously. As part of our ongoing commitment to the security of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards that further secure the information in our systems. We are also offering access to one year of credit monitoring and identity restoration services.

What You Can Do: While we are unaware of any attempted or actual misuse of your information contained within the affected accounts, we encourage you to consider taking action to protect yourself against any potential identity theft or fraud. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Prevent Fraud and Identity Theft*. There, you will also find more information on credit monitoring services and how to enroll in them.

For More Information: We understand that you may have questions about this incident that aren't addressed in this letter. If you have additional questions, please call our dedicated assistance line at 877-550-0353, Monday through Friday from 9 a.m. to 9 p.m. Eastern Time (excluding U.S. holidays).

Again, the National Restaurant Association takes the privacy and security of your information very seriously. We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

A handwritten signature in black ink that reads "Kevin Steele". The signature is written in a cursive style with a large initial "K" and a long, sweeping underline.

Kevin Steele
Chief Information Officer

STEPS YOU CAN TAKE TO PREVENT FRAUD AND IDENTITY THEFT

Enroll in Credit Monitoring:

As an added precaution, we have arranged for you to enroll, at no cost to you, in an online credit-monitoring service (*myTrueIdentity*) for one year, provided by TransUnion Interactive, a subsidiary of TransUnion®, one of three nationwide credit reporting companies.

To enroll in this service, go to the *myTrueIdentity* website at www.mytrueidentity.com. In the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code <<**Insert Unique 12- letter Activation Code**>> and follow the three steps to receive your credit-monitoring service online within minutes. Even if you are enrolled in credit-monitoring services with another vendor, you can still take advantage of this complimentary offer. Please utilize these instructions to enroll in the *myTrueIdentity* credit monitoring services.

If you do not have access to the Internet and wish to enroll in a similar, offline, paper based, credit-monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code <<**Insert static 6-digit Telephone Pass Code**>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<**Insert Date**>>. Because of privacy laws, we cannot register you directly. Please note that credit monitoring services may not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and valid Social Security number. Enrolling in this service will not affect your credit score.

Once enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit-monitoring service will notify you if there are any critical changes to your credit file, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised, to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Monitor Your Accounts:

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit-reporting bureaus. To order your free report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity before granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert or have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

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

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Security Freeze. You can also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without his or her written authorization. Please be advised, however, that placing a security freeze on your credit report might delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. If you have been a victim of identity theft and provide the credit bureau with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

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

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

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
[www.transunion.com/credit-freeze/
place-credit-freeze](http://www.transunion.com/credit-freeze/place-credit-freeze)

Additional Information: You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland residents, contact the Maryland Attorney General at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. Consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance received based on information in your credit report; and you may seek damages from the violator. You may also have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Rhode Island residents, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. Two Rhode Island residents may have been impacted by this incident.