



MULLEN  
COUGHLIN<sub>LLC</sub>

RECEIVED

JUN 19 2017

CONSUMER PROTECTION

Jim E. Prendergast  
Office: 267-930-4798  
Fax: 267-930-4771  
Email: [jprendergast@mullen.law](mailto:jprendergast@mullen.law)

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

June 13, 2017

**INTENDED FOR ADDRESSEE(S) ONLY**

**VIA U.S. MAIL**

Attorney General Joseph Foster  
Office of the New Hampshire Attorney General  
Attn: Security Breach Notification  
33 Capitol Street  
Concord, NH 03301

Re: Notice of Data Event

Dear Mr. Foster:

We represent Parkhurst Dining, 285 E. Waterfront Drive, Homestead, PA 15120, and are writing to notify your office of an incident that may affect the security of personal information relating to one (1) New Hampshire resident. By providing this notice, Parkhurst Dining does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

On April 20 2017, Parkhurst Dining learned that a Parkhurst Dining team member had clicked on a phishing email and entered their credentials. The team member's email account was immediately secured and Parkhurst Dining launched an in-depth investigation to determine whether any sensitive Parkhurst Dining information was accessed or acquired.

On May 16, 2017, Parkhurst Dining determined, with the help of outside computer forensic investigators, that an unknown actor had gained access to the Parkhurst Dining team member's email account. Parkhurst Dining determined, after a lengthy programmatic and manual review of the contents of the email account, the types of protected information contained in the email account and to which individuals the information relates on May 25, 2017, and immediately launched a review of its files to ascertain address information for its impacted individuals.

[Mullen.law](http://Mullen.law)

The email account may have contained the name, date of birth, address, Social Security Number, and financial account information, of the affected New Hampshire residents.

### **Notice to New Hampshire Resident**

On June 13, 2017, Parkhurst Dining. will begin providing written notice of this incident to all affected individuals, which includes approximately one (1) New Hampshire resident. 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**

Parkhurst Dining is providing all potentially affected individuals access to 2 free years of credit and identity monitoring services, including identity restoration services, through Kroll, and has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, Parkhurst Dining 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, information on protecting against tax fraud, 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. Parkhurst Dining is also providing written notice of this incident to other state regulators as necessary.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4798.

Very truly yours,



James E. Prendergast of  
MULLEN COUGHLIN LLC

JEP

# Exhibit A

## PRIVACY SAFEGUARDS INFORMATION

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two (2) years. Your identity monitoring services include:

### Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

### Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. 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.

### Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms 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 credit report, visit [www.annualcreditreport.com](http://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.

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 prior to 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 should you 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](http://www.equifax.com)

#### Experian

P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

#### TransUnion

P.O. Box 2000  
Chester, PA 19022-2000  
800-680-7289  
[www.transunion.com](http://www.transunion.com)

You may 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 the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may 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 you 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. 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. 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  
(NY residents please call  
1-800-349-9960)  
[www.freeze.equifax.com](http://www.freeze.equifax.com)

#### Experian Security Freeze

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/  
center.html](http://www.experian.com/freeze/center.html)

#### TransUnion

PO Box 2000  
Chester, PA 19022-2000  
1-888-909-8872  
[www.transunion.com/  
securityfreeze](http://www.transunion.com/securityfreeze)

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, 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](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and [www.oag.state.md.us](http://www.oag.state.md.us). **For North Carolina residents**, the 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](http://www.ncdoj.gov). Customers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, customers will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed as a result of a law enforcement investigation.



<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<ZipCode>>

**Re: Notice of Data Breach**

Dear <<MemberFirstName>> <<MemberLastName>>,

I am writing to let you know about a recent event that may affect the security of your personal information. Within this letter you will find the details about what happened as well as the steps we are taking in response, and steps you can take to protect against fraud should you feel it is appropriate.

I want to let you know that **we are unaware of any actual or attempted misuse of your personal information**, but out of an abundance of caution, we are providing you with detailed information about what happened. We care very much about the security of your personal information and about your peace of mind. It's our hope that this letter answers any potential concerns you may have. And, if not, we'll connect you with the appropriate resources to answer any additional concerns you may have.

**What Happened?** On April 20 2017, we learned that a Parkhurst Dining team member had clicked on a phishing email and entered their credentials. The team member's email account was immediately secured and Parkhurst Dining launched an in-depth investigation with the help of an outside computer forensic investigator to determine whether any sensitive Parkhurst Dining information was accessed or acquired.

Through that investigation, on May 16, 2017, we determined that an unknown actor had gained access to the Parkhurst Dining team member's email account. We then launched an in-depth and lengthy review of the specific contents of that email account. On May 25, Parkhurst Dining determined the types of protected information contained in the email account and to which individuals the information relates. We then immediately began a thorough review of the files to ascertain address information for the impacted individuals.

**What Information Was Involved?** As mentioned above, we currently have no evidence that the unauthorized individual or individuals has misused your information. But, we have confirmed that your <<ClientDef1 "Social Security number, date of birth, medical information, drivers license number, bank account number, benefits election form, benefits enrollment form, birth certificate, state identification number, credit card number, and passport number">> were accessible to the unknown actor.

**What We Are Doing.** We take the security of your information, and all information in our care, very seriously. We have been working diligently with third-party forensic investigators to determine what happened and what information was accessible to the unknown actor. This has involved a time consuming programmatic and manual data review process. We are providing notice of this event to you, and also to certain regulators and consumer reporting agencies as required. In addition to the steps taken above, we are providing you with additional information on how to better protect against identity theft and fraud. We have secured the services of Kroll to provide identity monitoring at no cost to you for two (2) years. Kroll is a global leader in risk mitigation and response and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Identity Consultation, and Identity Restoration. More information regarding these services can be found on the enclosed Privacy Safeguards. To enroll in the services being offered to you:

Visit [krollbreach.idMonitoringService.com](http://krollbreach.idMonitoringService.com) to activate and take advantage of your identity monitoring services. You have until September 14, 2017 to activate your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-844-263-8605. Additional information describing your services is included with this letter.

**What You Can Do.** You can activate the complimentary monitoring and restoration services we are offering to you. You can also review the enclosed Privacy Safeguards Information for additional information on how to better protect against identity theft and fraud.

**For More Information.** We are very sorry that this occurred and we apologize for any inconvenience this has caused you. The security of your information is a top priority for us, and we work hard to avoid incidents such as this one. Should you have any questions about the content of this letter or ways you can better protect yourself from the possibility of identity theft, we encourage you to call the dedicated assistance line, staffed by professionals who are experienced in working through situations like this, at 1-866-775-4209 between 9:00 a.m. and 6:00 p.m. ET, Monday through Friday, excluding major holidays.

Sincerely,

A handwritten signature in cursive script that reads "Karen B. Bolden".

Karen Bolden  
Chief People Officer  
Parkhurst Dining