



MULLEN
COUGHLIN_{LLC}

STATE OF NH
DEPT. OF JUSTICE

2019 JAN -7 P 3:06

James E. Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

January 2, 2019

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 Attorney General MacDonald:

We represent Hankin Group, 707 Eagleview Blvd, Exton, PA 19341, and write to provide notice to your office of an incident that may affect the security of personal information relating to a certain New Hampshire resident. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Hankin Group does not waive any rights or defenses regarding the applicability of New Hampshire law, the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about November 19, 2018, Hankin Group identified suspicious email activity within an employee's email account. Upon learning of this suspicious email activity, Hankin Group promptly launched an internal investigation with the assistance of third-party forensic investigators. Through this investigation, on or about November 27, 2018, Hankin Group confirmed there was unauthorized access to an employee email account between October 31, 2018 and November 19, 2018.

On or about December 10, 2018, as the result of a thorough review of the potentially exposed contents of the impacted email account, the investigation confirmed the population of potentially impacted individuals. The types of potential personal information impacted in relation to this incident include the following: name, date of birth, Social Security number, and/or financial account number. Beginning on December 10, 2018, Hankin

Group took steps to identify the address information necessary for providing notification to the affected individuals.

Notice to New Hampshire Resident

On January 2, 2019, Hankin Group began mailing written notice of this incident to the affected individuals, including one (1) New Hampshire resident. Written notice will be provided in substantially the same form as the letter attached hereto as *Exhibit A*.

Other Steps Taken and to Be Taken

Upon discovering this incident, Hankin Group promptly began an investigation with the assistance of a third-party forensic investigator to determine the nature and scope of this incident, including identifying the individuals who may be affected, putting in place resources to assist them, and providing them with notice of this incident. Hankin Group identified and mitigated the incident by ensuring the password for the affected email account was changed. Hankin Group has also taken additional actions to strengthen the security of its email systems, as well as providing additional training to users on how to identify phishing scams.

Hankin Group is providing potentially affected individuals access to 24 months of credit monitoring and identity restoration services through TransUnion. Additionally, Hankin Group 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 identity theft and fraud 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. Hankin Group is also notifying other state regulators, as required.

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

EXHIBIT A

<<Company Name>>
Return Mail Processing Center
P.O. 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>>

Dear <<Name 1>>:

<<Company Name>> recently discovered an incident that may affect the security of your personal information. We write to provide you with information about the incident, steps we are taking in response, and steps you can take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? On or about November 19, 2018, <<Company Name>> identified suspicious email activity within an employee's email account. Upon learning of this suspicious email activity, <<Company Name>> promptly launched an internal investigation with the assistance of third-party forensic investigators. Through this investigation, on or about November 27, 2018, <<Company Name>> confirmed there was unauthorized access to an employee email account between October 31, 2018 and November 19, 2018.

What Information Was Involved? On or about December 10, 2018, after a thorough review process, <<Company Name>> confirmed the impacted email account contained, and the unauthorized actor may have accessed, the following personal information related to you: <<Data Elements>>. To date, we have no evidence of any actual or attempted misuse of the information impacted by this incident.

What Are We Doing? We take this incident and the security of your personal information seriously. <<Company Name>> identified and mitigated the issue by ensuring the password for the affected email account was changed. We are also taking additional actions to strengthen the security of our email systems, as well as providing additional training to users on how to identify phishing scams.

We are providing you with information you can use to better protect against identity theft and fraud, as well as access to 24 months of complimentary credit monitoring and identity restoration services with TransUnion. Instructions for enrolling in the credit monitoring services, as well additional information on how to better protect against identity theft or fraud, are included in the attached *Privacy Safeguards*.

What Can You Do? You can review the *Privacy Safeguards* for additional information on how to better protect against potential identity theft and fraud. You can also enroll to receive the complimentary credit monitoring and identity restoration services described above.

For More Information. We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call our toll-free dedicated assistance line at 877-854-8723. This toll-free line is available Monday through Friday from 9:00 am to 9:00 pm EST, excluding major national holidays. We apologize for any inconvenience or concern this incident causes you.

Sincerely,

A handwritten signature in black ink, appearing to read "Michael Hankin". The signature is fluid and cursive, with a large initial "M" and "H".

Michael Hankin
Chief Operating Officer

Enclosure

PRIVACY SAFEGUARDS

Enroll in Credit Monitoring.

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

How to Enroll: You can sign up online or via U.S. Mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based, three-bureau 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 six-digit telephone passcode <<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 <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might 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 a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score.
- The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian®, and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes 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 and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Monitor Your Accounts.

We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your 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 credit 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.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872

www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

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

www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

For More Information. You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, 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); 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be promptly reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, North Carolina residents may wish to review information provided by the North Carolina Attorney General, Consumer Protection Division at www.ncdoj.gov, by calling 877-566-7226, or writing to 9001 Mail Services Center, Raleigh, NC 27699.