



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

OCT 24 2017

CONSUMER PROTECTION

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

1275 Drummers Lane, Suite 302
Wayne, PA 19087

October 20, 2017

VIA US 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 Security Incident

Dear Mr. MacDonald:

We represent LightHouse Management Services, LLC, d/b/a Home Properties (“Home Properties”), 300 Clinton Square, Rochester, NY 14604, and are writing to notify you of a data security incident that may have affected the security of information related to certain individuals residing in and businesses operating in New Hampshire. Home Properties reserves the right to supplement this notice with any new significant facts learned subsequent to its submission. By providing this notice, Home Properties does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data breach notification statute, or personal jurisdiction.

Nature of the Data Event

On or about July 19, 2017, Home Properties learned of suspicious activity related to an employee’s email account. Upon learning of this suspicious activity, Home Properties immediately initiated an internal investigation and also hired a third-party forensic investigator to determine the nature and scope of the incident, including whether any sensitive information was affected. Through this investigation, Home Properties determined that the employee’s email account may have been accessed without authorization between July 19, 2017 and July 26, 2017.

On or around September 26, 2017, Home Properties determined that the affected email account contained, and the unauthorized individual may have had access to, the following information: name, address, telephone number, email address, date of birth, Social Security number, driver’s license or state identification card number, bank account number, and/or credit card number.

While the investigation is ongoing, Home Properties does not currently have any evidence of actual or attempted misuse of personal information as a result of this incident.

Notice to New Hampshire Residents

On October 20, 2017, Home Properties will begin providing written notice of this incident to the affected individuals and businesses, which includes approximately two (2) individuals who reside in New Hampshire and one (1) business that operates in New Hampshire. Written notice will be provided in substantially the same form as the letters attached hereto as *Exhibit A* and *Exhibit B*.

Other Steps Taken and To Be Taken

After discovering the suspicious email activity, Home Properties, with the assistance of third-party forensic investigators, moved quickly to identify those who may be affected and to provide them with notice of this incident. Additionally, Home Properties promptly ensured that the affected employee's password was changed, and continues to monitor their systems to ensure the privacy and security of personal information.

Home Properties is providing all potentially affected individuals access to 36 months of complimentary credit monitoring and identity restoration services, through AllClear ID. Additionally, Home Properties is providing potentially impacted individuals and businesses 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.

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:am

Enclosure

Exhibit A

[Home Properties Logo/Letterhead]

[Date]

[Name]

[Street Address]

[City], [State] [Zip Code]

Re: Notice of Data Breach

Dear [Name]:

Home Properties 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 July 19, 2017, Home Properties learned of suspicious activity related to an employee's email account. Upon learning of this suspicious activity, Home Properties immediately initiated an internal investigation and also hired a third-party forensic investigator to determine the nature and scope of the incident, including whether any sensitive information was affected. Through this investigation, Home Properties determined that the employee's email account had been accessed without authorization between July 19, 2017 and July 26, 2017.

What Information Was Involved? On or around September 26, 2017, Home Properties determined that the affected email account contained, and the unauthorized individual may have had access to, the following information related to you: name, address, telephone number, email address, date of birth, driver's license number or state identification card number, bank account number, and/or credit card number. While our investigation is ongoing, we do not currently have any evidence of actual or attempted misuse of your information.

What We Are Doing. We take this incident and the security of your personal information very seriously. In addition to hiring a third-party forensic investigator to conduct an investigation, we have also ensured that all employees who received the phishing email changed their passwords, and we continue to monitor our systems to ensure the privacy and security of your personal information. We are also providing you with information you can use to better protect against identity theft and fraud, as well as access to 36 months of credit monitoring and identity restoration services with AllClear ID at no cost to you. You can find more information and steps you can take, as well as information on how to enroll in the credit monitoring services, in the enclosed *Privacy Safeguards Information*.

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

For More Information. We sincerely regret any inconvenience or concern this incident causes you. We understand that you may have questions that are not addressed in this notice. If you have additional questions, please contact Dorothy Cooper at 1-(585) 246-4188.

Sincerely,

[Signature]

[Signatory Name]

[Signatory Title]

Enclosure

PRIVACY SAFEGUARDS INFORMATION

Enroll in Credit Monitoring. As an added precaution, we have arranged to have AllClear ID protect your identity for 36 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 36 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-866-979-2595 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-866-979-2595 using the following redemption code: [Redemption Code].

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

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 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.

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 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

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

TransUnion
P.O. Box 2000
Chester, PA 19016
800-680-7289
www.transunion.com

Security Freeze. 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. 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

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 that 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.

Exhibit B

[Home Properties Logo/Letterhead]

[Date]

[Name]

[Street Address]

[City], [State] [Zip Code]

Dear [Name]:

Home Properties recently discovered an incident that may affect the security of your company's 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 potential misuse of your company's information, should you feel it is appropriate to do so.

What Happened? On or about July 19, 2017, Home Properties learned of suspicious activity related to an employee's email account. Upon learning of this suspicious activity, Home Properties immediately initiated an internal investigation and also hired a third-party forensic investigator to determine the nature and scope of the incident, including whether any sensitive information was affected. Through this investigation, Home Properties determined that the employee's email account had been accessed without authorization between July 19, 2017 and July 26, 2017.

What Information Was Involved? On or around September 26, 2017, Home Properties determined that the affected email account contained, and the unauthorized individual may have had access to, the following information related to your company: name, address, employer identification number (EIN), bank account number and/or credit card number. While our investigation is ongoing, we do not currently have any evidence of actual or attempted misuse of your information.

What We Are Doing. We take this incident and the security of your company's information very seriously. In addition to hiring a third-party forensic investigator to conduct an investigation, we have also ensured that all employees who received the phishing email changed their passwords, and we continue to monitor our systems to ensure the privacy and security of your company's information. We are also providing you with information you can use to better protect against the potential misuse of your company's information. You can find more information and steps you can take in the enclosed *Privacy Safeguards Information*.

What You Can Do. Please review the enclosed *Privacy Safeguards Information* for additional information on how to better protect against the potential misuse of your company's information.

For More Information. We sincerely regret any inconvenience or concern this incident causes you and your company. We understand that you may have questions that are not addressed in this notice. We understand that you may have questions that are not addressed in this notice. We understand that you may have questions that are not addressed in this notice. If you have additional questions, please contact Dorothy Cooper at 1-(585) 246-4188.

Sincerely,

[Signature]

[Signatory Name]

[Signatory Title]

Enclosure

PRIVACY SAFEGUARDS INFORMATION

Monitor Your Accounts. We encourage you to remain vigilant against incidents of identity theft and financial loss by reviewing your company's account statements for suspicious activity. Should you suspect any suspicious activity in a bank or financial account, we encourage you to contact your bank or financial institution and discuss the matter with them.

While companies do not have credit files, the following information relates to protecting an individual's credit:

Monitor Your Accounts.

Credit Reports. 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.

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 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

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 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. 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

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 that 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.