



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

April 6, 2021

Michael J. Waters
312-463-6212
312-819-1910 Direct Fax
mwaters@polsinelli.com

Via Email (ATTORNEYGENERAL@DOJ.NH.GOV)

Office of the Attorney General
Attn: Security Incident Notification
33 Capitol Street
Concord, NH 03301

Re: Notification of a Computer Security Incident Involving Personal Information Pursuant to N.H. Rev. Stat. § 359-C:20

To whom it may concern:

We represent Lincoln Property Company (“Lincoln”) in connection with an incident that may have impacted the personal information of one (1) New Hampshire resident, and provide this notice on behalf of Lincoln pursuant to N.H. Rev. Stat. § 359-C:20(I)(b). We will supplement this notice, if necessary, with any new significant facts discovered subsequent to its submission. While Lincoln is notifying you of this incident, Lincoln does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE SECURITY INCIDENT

Lincoln recently discovered an attempted cyberattack on some of its computer systems. Lincoln has proactive security tools in place that helped it discover and stop the attempted attack. Upon discovering the incident, Lincoln promptly conducted an internal investigation, and engaged a leading forensic firm to investigate and confirm the security of Lincoln’s network. The forensic investigation determined an unknown, unauthorized third party accessed Lincoln’s network for a short period of time on November 17, 2020. The forensic firm found no evidence that the unknown third party’s motive was to obtain personal information, and Lincoln is not aware of any attempt or actual misuse of such personal information. Nevertheless, because an unknown third party had unauthorized access to Lincoln’s network and Lincoln could not conclusively rule out the possibility that certain documents were obtained, it reviewed those documents that could have been acquired and determined that they included some personal information.

polsinelli.com

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



April 6, 2021
Page 2

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

On or about March 12, 2021, Lincoln determined that one (1) New Hampshire resident may have been involved in this incident. Lincoln is notifying the resident of the situation by letter today, April 6, 2021. The notification letter also includes an offer for twelve (12) months of complimentary credit monitoring and identity theft protection. Enclosed is a copy of the notice that is being sent to the New Hampshire resident via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, Lincoln promptly controlled the incident by preventing any further access to its network. Further, Lincoln engaged a leading forensic firm to investigate and confirm the security of its network. Lincoln is undertaking efforts to reduce the risk of a similar incident occurring in the future, including enhancing its technical security measures. Finally, as discussed above, Lincoln is notifying impacted individuals and providing them with information on how they can protect themselves against fraudulent activity and identity theft.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

A handwritten signature in black ink, appearing to read "Michael J. Waters".

Michael J. Waters

Enclosure



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

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

RE: NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Lincoln Property Company values and respects the privacy of your information, which is why we are writing to advise you of a recent incident that may have involved some of your personal information. We have no reason to believe that your personal information has been acquired or misused. Nonetheless, we are writing to advise you about the incident and to provide you with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened? We recently discovered an attempted cyberattack on some of our computer systems. We have proactive security tools in place that helped us discover and stop the attempted attack. In the course of our investigation into the incident, we came to learn that someone accessed certain areas of our network for a short period of time. We do not believe that this was done in an attempt to acquire anyone's information and we have no evidence that anyone's information was accessed. Nevertheless, because someone had access to those areas and we could not conclusively rule out the possibility that certain documents were obtained, we reviewed those documents and determined that they included some of your information.

What Information Was Involved? On March 12, 2021, we determined that the documents that could have been accessed contained personal information that included your name and Social Security number.

What We Are Doing. Upon discovering the situation, we engaged a leading forensic security firm to conduct an investigation of the incident and confirm the security of our network. Upon determining that the third party had access to personal information, we worked to locate current contact information and notify individuals as quickly as possible. We have also taken steps to reduce the risk of this type of incident occurring in the future.

What You Can Do. 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. IdentityWorks Credit 3B is completely free to you, and enrolling in this program will not hurt your credit score. **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.**

Other Important Information. You can find more information on steps to protect yourself against identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information. We value the trust you place in us to protect your privacy and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call 1-855-935-6087 from 8:00 a.m. – 5:30 p.m. Central, Monday through Friday.

Sincerely,

Lincoln Property Company

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(EnrollmentDeadline)>> (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 877-288-8057. Be prepared to provide engagement number <<b2b_text_2(EngagementNumber)>> 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** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$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 877-288-8057 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 877-288-8057.

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

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. 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 can be placed without any charge and 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 1-888-298-0045 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
---	--	---

This notification was not delayed by law enforcement.

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/bcftp_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.

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, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

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.

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, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.