MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

March 12, 2024

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent BuildingLink.com, LLC ("BuildingLink"), located at 85 5th Ave, Floor 3, New York, NY 10003, and are writing to notify your Office of an incident that may affect the security of information relating to certain New Hampshire resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, BuildingLink 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

In September 2022, BuildingLink discovered that computer systems were infected with a virus that encrypted certain systems. Upon discovery, BuildingLink immediately notified law enforcement and began an investigation, which included working with third-party forensic investigators, to determine the full nature and scope of the incident and to secure the BuildingLink network. This investigation determined that certain BuildingLink systems were subject to unauthorized access on or about August 28, 2022. BuildingLink then undertook a manual review of the impacted data set in order to determine the data that could have been accessed by the unauthorized actor and to identify address information in order to provide them with notice of this event. While the information varies for each individual, this comprehensive review confirmed that may have been present in the affected systems at the time of the incident.

Notice to New Hampshire Resident

On or about March 8, 2024, BuildingLink provided written notice of this incident to one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, BuildingLink moved quickly to investigate and respond to the incident, assess the security of BuildingLink systems, and identify potentially affected individuals. Further, BuildingLink notified federal law enforcement regarding the event. BuildingLink is also working to implement additional safeguards and training to its employees. BuildingLink is providing access to complimentary credit monitoring services for , through Kroll, to individuals whose information was potentially affected by this incident.

Additionally, BuildingLink is providing impacted individuals with guidance on how to better protect against identity theft and fraud, 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 event, please contact us at .

Very truly yours,

Gregory Lederman of
MULLEN COUGHLIN LLC

GCL/jrl
Enclosure

EXHIBIT A

BuildingLink

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

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

BuildingLink.com, LLC ("BuildingLink") writes to inform you of an incident that may affect the security of some of your information. The confidentiality, privacy, and security of our employees' information in BuildingLink's care is one of its highest priorities and we take this incident very seriously. Although we have not received any reports of actual or attempted misuse of information as a result of this event, we are providing this notice in an abundance of caution and are providing information about the incident, our response, and steps you can take to help protect your information, should you feel it is appropriate to do so.

What Happened? In September 2022, BuildingLink discovered that certain systems were infected with a virus that encrypted certain systems. Upon discovery, BuildingLink immediately notified law enforcement and began an investigation, which included working with third-party forensic investigators, to determine the full nature and scope of the incident and to secure the BuildingLink network. This investigation determined that certain BuildingLink systems were subject to unauthorized access on or about August 28, 2022. As a result, this information may have been accessed or acquired by the unauthorized actor. BuildingLink took steps to complete a thorough review of the data that could have been accessed by the unauthorized actor.

What Information Was Involved? BuildingLink recently completed a manual review of the information which may have been accessed or acquired as a result of this incident, and a search of records to identify addresses for all impacted individuals. BuildingLink is notifying you because this review confirmed that your may have been present in the affected systems at the time of the incident.

What Are We Doing? BuildingLink reiterates that we take the confidentiality and security of information it our care very seriously. Upon learning of this incident, we immediately launched an investigation, took steps to secure BuildingLink systems, and began a review to determine what information was potentially at risk. As part of our ongoing commitment to the security of information in our care, we continue to review our existing policies and procedures, to implement additional safeguards, and to provide additional training to employees on data privacy and security. We will also be notifying regulators, as required.

As an added precaution, we are also offering you complimentary access to of credit monitoring and identity theft restoration services, through Kroll. We encourage you to activate these services, as we are not able to act on your behalf to activate them for you. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What Can You Do. We encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information* for additional steps you may take and information on what you can do to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so. You may also activate the complimentary credit and identity monitoring services we are offering.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions about this incident, please call BuildingLink's dedicated assistance line at XXX-XXX-XXXX, Monday through Friday between the hours 8:00 am and 5:30 pm Central Time.. You may also write to BuildingLink at 85 5th Ave, Floor 3, New York, NY 10003.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

BuildingLink

Steps You Can Take to Help Protect Your Information

Activate Identity and Credit Monitoring Services

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 one year. 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, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 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 reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

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 will be able to help you determine if it is 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.