MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

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

November 27, 2023

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 The Beacon Insurance Services ("Beacon") located at 120 South Warner Road, Suite 201, King of Prussia, PA 19406, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) New Hampshire resident. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Beacon 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 February 3, 2023, Beacon became aware of suspicious activity related to an employee's email account. Beacon immediately took steps to secure the employee's email account and launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that an unknown actor logged into one employee's email account without authorization between January 31, 2023, and February 3, 2023.

There was no indication found that sensitive personal information stored within the impacted email account was specifically targeted, and Beacon is not aware of any identity theft or fraud relating to this incident at this time. However, in an abundance of caution, Beacon conducted a thorough and time-intensive review of the contents of the impacted email account to identify sensitive information stored therein, to whom it relates, and the Beacon client to whom the individual belonged. This review concluded recently, and Beacon moved quickly to notify both individuals and customer business entities on behalf of whom Beacon handled personal information within the impacted email account. Where Beacon identified potentially impacted personal information sourced from its customer business entities, it has offered to provide notice to individuals on behalf of the customer business entities.

The information that could have been subject to unauthorized access includes .

Notice to New Hampshire Resident

On October 16, 2023, Beacon mailed written notice of this incident to 133 customer business entities to disclose the incident and offer to mail notice of the incident to individuals affiliated with the businesses. On or about November 27, 2023, Beacon began mailing written notice 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, Beacon moved quickly to investigate and respond to the incident, assess the security of Beacon's email tenant, and identify potentially affected individuals. Beacon is also working to review existing security policies and implementing additional safeguards and training to its employees. Beacon is providing access to credit monitoring services for twelve (12) months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Beacon is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Beacon is providing individuals with 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.

Beacon is providing written notice of this incident to relevant 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 .

Very truly yours,

Alexander T. Walker of
MULLEN COUGHLIN LLC

ATW/jlm
Enclosure

EXHIBIT A

Return Mail to IDX
4145 SW Watson Ave
Suite 400
Beaverton, OR 97005

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

November 27, 2023

NOTICE OF <<SECURITY INCIDENT/DATA BREACH>>

Dear <<Name 1>> <<Name 2>>:

Beacon Insurance Services ("Beacon") is providing you this notification on behalf of <<Variable 2>> to make you aware of an event that may impact the security of some of your personal information. Beacon is an insurance agency that assists client businesses with the acquisition and administration of commercial and automobile insurance. This letter provides details of the event, our ongoing response, and steps you can take to further secure your information, should you feel it necessary to do so.

What Happened?

On February 3, 2023, Beacon became aware of suspicious activity related to an employee's email account. We immediately took steps to secure the employee's email account and launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that an unknown actor logged into one employee's email account without authorization between January 31, 2023 and February 3, 2023.

There was no indication found that sensitive personal information stored within the impacted email account was specifically targeted, and we are not aware of any identity theft or fraud relating to this incident at this time. However, in an abundance of caution, we conducted a thorough and time-intensive review of the contents of the impacted email account to identify sensitive information stored therein and to whom it relates.

What Information Was Involved?

The following types of your information were determined to be stored in the impacted email account: <<DATA ELEMENTS>> and name. Please note, we are not aware of any identity theft or fraud relating to this incident at this time.

What We Are Doing.

Information security is among our highest priorities. Upon becoming aware of this incident, Beacon took steps to secure the email account and immediately launched an investigation into the nature and scope of the event. We are also reviewing existing security policies and implementing additional cybersecurity measures to further protect against similar incidents moving forward. Additionally, Beacon is revamping its employee training program and notifying individuals and relevant regulators of this event, as required.

As an added precaution, we are offering you immediate access to credit monitoring and identity theft protection services for <<12/24>> months at no cost to you, through IDX. You can find information on how to enroll in these services in the below *Steps You Can Take to Further Protect Your Information.* We encourage you to enroll in these services as we are not able to do so on your behalf. Please note the deadline to enroll is February 27, 2024.

What You Can Do.

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 and to detect errors over the next 12 to 24 months. Please also review the information contained in the enclosed *Steps You Can Take to Further Protect Your Information.*

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, please call our dedicated assistance line at 1-888-819-7666, between the hours of 9 am to 9 pm Eastern Time, Monday through Friday. You may also write to Beacon at 120 South Warner Road, Suite 201, King of Prussia, PA 19406.

We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

The Beacon Group of Companies

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Enroll in Monitoring Services

1. Website and Enrollment. Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-888-819-7666 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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
1-888-298-0045	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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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, D.C. 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; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<#>> Rhode Island residents that may be impacted by this event.