Anjali C. Das
312.821.6164 (Direct)
anjali.das@wilsonelser.com

January 31, 2024

Via Online Submission

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker, LLP ("Wilson Elser") represents J.D. Gilmour & Co. ("J.D. Gilmour"), an insurance broker based in Glendale, California, with respect to a cybersecurity incident that was discovered by J.D. Gilmour on June 29, 2023 (hereinafter, the "Incident"). Please note J.D. Gilmour takes the security and privacy of the information within its control seriously, and has taken steps to prevent a similar incident from occurring in the future. This letter will serve as a notice of the Incident and to inform you of the steps J.D. Gilmour has taken in response to the Incident.

1. Nature of the Incident

On June 29, 2023, J.D. Gilmour became aware of potential unauthorized access to its e-mail environment (the "Incident"). Upon discovering the Incident, J.D. Gilmour immediately engaged a third-party cybersecurity forensic team to conduct a thorough investigation into its entire e-mail tenant and determine the nature and scope of the Incident. On August 8, 2023, the forensic investigation determined that an unknown party had gained unauthorized access to one (1) J.D. Gilmour employee e-mail user account.

Based upon this finding, J.D. Gilmour engaged a third-party data mining vendor to review the data within the compromised e-mail user account and determine whether sensitive information was maintained therein at the time of the Incident. On October 27, 2023, J.D. Gilmour completed its investigation of the data maintained within the compromised e-mail user account and determined

System.Object[]

that sensitive personal information in relation to health insurance was impacted as a result of the Incident.

Subsequently, J.D. Gilmour conducted a review of those individuals whose information was impacted as a result of the Incident to determine which insurance providers were associated with the affected individuals. Based upon its review, J.D. Gilmour notified the various health insurance companies associated with the affected individuals to obtain authorization to provide notification of the Incident. Upon receiving authorization from various health insurance companies, J.D. Gilmour mailed notice letters to those individuals affected by the Incident.

Please note that, to date, the investigation has found no evidence of actual or attempted misuse of personal information as a result of this incident.

2. Number of Maine residents affected.

J.D. Gilmour discovered that the Incident may have resulted in unauthorized exposure of information pertaining to one (1) Maine resident. A notification letter to the affected individual was mailed on January 16, 2024, by First Class Mail. A sample copy of the notification letter is attached hereto as **Exhibit A**.

3. Steps taken in response to the Incident.

J.D. Gilmour is committed to ensuring the security and privacy of all personal information within its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, engaged a specialized cybersecurity firm to conduct a forensic investigation in order to determine the nature and scope of the Incident. Additionally, J.D. Gilmour has taken steps to strengthen its security posture to prevent a similar event from occurring again in the future.

J.D. Gilmour is also offering twelve (12) months of complimentary credit monitoring and identity theft restoration services through Cyberscout through Identity Force, a TransUnion company, to potentially affected individuals residing in Maine to help protect their identity. Additionally, J.D. Gilmour provided guidance on how to better protect against identity theft and fraud, including providing 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 and Federal Trade Commission, information on how to obtain a free credit report, and a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports.

4. Contact Information

J.D. Gilmour remains dedicated to protecting the sensitive information within its control. Should you have any questions or need additional information, please do not hesitate to contact me at anjali.das@wilsonelser.com or 312.821.6164.

Very truly yours,

WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

Anjali C. Das

EXHIBIT A

JD Gilmour
c/o Cyberscout
1 Keystone Ave, Unit 700
Cherry Hill, NJ 08003
DB08374 1-1

J.D. GILMOUR & CO.
INSURANCE SERVICES

[redacted]

January 16, 2024

Notice of Data Breach

Dear [redacted],

J.D. Gilmour is writing to notify you of a recent data security incident that may have involved your personal information. J.D. Gilmour takes the security of personal information very seriously, and we apologize for any inconvenience this incident may cause. This letter contains additional information about the incident, our response to this Incident, and steps you can take to safeguard your information.

What Happened:

On June 29, 2023, J.D. Gilmour became aware of a potential unauthorized access to its e-mail environment (the "Incident"). Upon discovering the Incident, J.D. Gilmour immediately engaged a third-party cybersecurity forensic team to conduct a thorough investigation into its entire e-mail tenant and determine the nature and scope of the Incident. On August 8, 2023, the forensic investigation determined that an unknown party had gained unauthorized access to one (1) J.D. Gilmour employee e-mail user account.

Based upon this finding, J.D. Gilmour engaged a third-party data mining vendor to review the date within the compromised e-mail user account and determine whether sensitive information was maintained therein during the time of the Incident. On October 27, 2023, J.D. Gilmour completed its investigation of the data maintained within the compromised e-mail user account and determined that your personal information in relation to your coverage with [redacted] was impacted as a result of the Incident. Subsequently, J.D. Gilmour notified [redacted] that individuals associated with its organization were determined to have been impacted by the Incident and obtained authorization to notify you of the Incident. On December 21, 2023, [redacted] authorized J.D. Gilmour to notify its members affected by the Incident on its behalf.

Please note that to date, the investigation has found no evidence of actual or attempted misuse of personal information as a result of this incident.

What Information Was Involved:

Based upon the results of the investigation, J.D. Gilmour determined that the elements of your personal information that were exposed may have included your: [redacted].

Please note that there is no evidence at this time that any of your personal information has been misused as a result of this incident.

What We Are Doing:

We are working with cybersecurity experts to determine the actions to take in response to the incident. Together, we continue to investigate and closely monitor the situation. Further, we are taking steps to strengthen our security posture to prevent a similar event from occurring again in the future.

As a safeguard, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. 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, 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.

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/jdgilmour** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

We encourage you to remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Additionally, we recommend that you review the following page, which contains important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

For More Information:

Please know that the protection of your personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 1-833-892-4287 Monday – Friday, 8:00 am to 8:00 pm Eastern Time, excluding holidays.

Sincerely,

J.D. Gilmour

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us
Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov
North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com
Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft
New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft
For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:
Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.
Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.
Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
equifax.com/personal/credit-report-services/	experian.com/freeze/center.html	transunion.com/credit-freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.