Lynda Jensen
Office: (267) 930-2303
Fax: (267) 930-4771
Email: Ljensen@mullen.law

3 Allied Drive, Suite 303
Dedham, MA 02026

March 1, 2022

VIA E-MAIL ONLY

Montana Department of Justice
Office of Consumer Protection
P.O. Box 200151
Helena, MT 59620-0151
E-mail: ocpdatabreach@mt.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent LGAA, LLC ("LGAA") located at 136 W. University Blvd., Cedar City, UT 84720, and are writing to notify your office of an event that may affect the security of some personal information relating to approximately eleven (11) Montana residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, LGAA does not waive any rights or defenses regarding the applicability of Montana law, the applicability of the Montana data event notification statute, or personal jurisdiction.

Nature of the Data Event

In March 2021, while confirming the security of its systems in light of the Microsoft Zero-Day Exchange vulnerability, LGAA learned of possible unauthorized access to some of the data stored within its data center. LGAA's data center houses information for some of its affiliate agencies. Upon learning of the possible unauthorized access event, with the assistance of leading third-party cybersecurity specialists, an investigation was immediately launched to confirm the nature and scope of the potential event. The investigation determined that certain data relating to certain affiliate agency clients and plan participants might have been accessed without authorization between approximately February 16 and March 18, 2021. LGAA then engaged an industry-leading data analytics firm to conduct a thorough review to determine whether sensitive information was present in the impacted files and to whom that data relates. This time-consuming and labor-intensive review was completed on or about September 23, 2021. To locate missing address information for potentially affected individuals, as well as to determine to which data owners the potentially affected individuals relate, LGAA undertook an additional subsequent comprehensive internal review. This thorough and time-consuming review was completed on December 13, 2021. LGAA worked to quickly notify the affected data owners of this event. However, the reviews were unable to identify the

data owners for some of the potentially affected information. As such, in an abundance of caution, LGAA is notifying the identified individuals directly. The information that could have been subject to unauthorized access includes name, address, Social Security number, medical information, financial account information, health insurance information, and driver's license or state identification number.

Notice to Montana Residents

On or about March 1, 2022, LGAA provided written notice of this event to affected individuals for whom data owner information was unable to be identified through LGAA's comprehensive and time-consuming reviews, which includes approximately eleven (11) Montana residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. LGAA is also providing notice on its webpage and to media distribution outlets to ensure all potentially affected individuals are notified of this event.

Other Steps Taken and To Be Taken

Upon discovering the event, LGAA moved quickly to investigate and respond to the event, assess the security of LGAA systems, and notify the above referenced individuals. LGAA is also working to implement additional safeguards and training to its employees to further fortify its systems. LGAA is providing access to credit monitoring services for one (1) year, through IDX, to the potentially affected, at no cost to these individuals.

Additionally, LGAA 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. LGAA 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. Individuals were also provided with information on how to report suspicious information to appropriate insurance companies and healthcare providers.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-2303.

Very truly yours,

Lynda Jensen of
MULLEN COUGHLIN LLC

LRJ/dle
Attachment

Exhibit A

P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-774-1210
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<Enrollment>>

<<First Name>> <<MI>> <<Last Name>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

March 1, 2022

<<Variable1>>

Dear <<First Name>> <<MI>> <<Last Name>> <<Suffix>>:

LGAA, LLC ("LGAA") and some of its affiliate agencies (collectively, "Leavitt") are writing to inform you of an incident that may impact some of your information. Leavitt is comprised of insurance agencies and your information was provided to them as part of service and administration of that insurance. Leavitt is providing you with information about the incident, the response to that incident, and steps you may take to better protect your information, should you feel it is appropriate to do so.

What Happened? In March 2021, LGAA learned of possible unauthorized access to some of the data stored within its data center. Upon learning of the possible incident, with the assistance of a leading third-party cybersecurity investigation firm, an investigation was immediately launched to confirm the nature and scope of the potential unauthorized access. The investigation determined that certain data relating to certain Leavitt clients and plan participants might have been accessed by someone without authorization between approximately February 16 and March 18, 2021. LGAA then engaged an industry-leading data analytics firm to conduct a thorough review to determine whether sensitive information was present in the impacted files and to whom that data relates. This time-consuming and labor-intensive review was completed on or about September 23, 2021. To locate missing address information for potentially affected individuals, as well as to determine to which plan or employer the potentially affected individuals relates, Leavitt undertook an additional subsequent comprehensive internal review. This thorough and time-consuming review was completed on December 13, 2021. Leavitt quickly began notifying potentially affected individuals.

What Information Was Involved? Leavitt's investigation into the incident determined that certain data relating to clients and plan participants might have been subject to unauthorized access. However, the investigation was unable to determine to which affiliate agency or insurance plan your information relates. Necessarily, Leavitt is notifying you of this incident because the investigation confirmed that the accessible files contained information relating to you included your <<Variable2>>, and name.

What We Are Doing. Leavitt takes this incident very seriously. When Leavitt discovered this incident, it immediately secured the data center environment and took steps to determine what information was in the impacted files and to whom the information belonged. As part of the ongoing commitment to the security of information entrusted to our care, Leavitt is reviewing existing policies and procedures regarding information provided to them and implementing additional safeguards. Leavitt is also providing notice of this incident to state and federal regulators, as required.

Although there is no evidence of actual or attempted misuse of your information, as an added precaution, you are being offered complimentary access to <<12/24>> months of credit and identity monitoring services through IDX. We

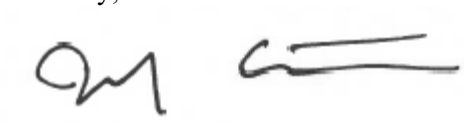
encourage you to activate these services, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What You Can Do. Leavitt encourages you to remain vigilant against potential incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity. You can find out more about how to safeguard your information in the enclosed *Steps You Can Take to Help Protect Your Information*, should you feel it appropriate to do so. You also may activate the free credit monitoring services we are offering.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please contact the dedicated call center at the toll-free number 1-833-774-1210, Monday through Friday from 8 am to 8 pm Central Time. You may also write to Leavitt at 136 W University Blvd, Cedar City, UT 84720.

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,



Joe Callister
President and CEO
LGAA, LLC

Steps You Can Take to Help Protect Your Information

Enroll in Credit Monitoring

1. **Website and Enrollment.** 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. Please note the enrollment deadline is June 1, 2022.

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 1-833-774-1210 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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You also may contact directly 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 one-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 credit 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
1-888-298-0045	1-888-397-3742	1-833-395-6938
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 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, D.C. 20001; 1-202-727-3400; 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 www.oag.state.md.us.

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 contacted at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed regarding this incident. There are three (3) Rhode Island residents impacted by this incident.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your 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 your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You 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 you to review your 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/.