Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

July 28, 2023

By Electronic Mail: *consumer_protection@ag.idaho.gov*

The Honorable Raúl Labrador
Attorney General's Office
Consumer Protection Division
P.O. Box 83720
Boise, ID 83720-0010

Re: Data Security Incident

Dear Attorney General Labrador:

We write on behalf of Maximus, Inc. and its subsidiaries (collectively, "Maximus"), with headquarters located at 1600 Tysons Blvd, McLean, VA 22102, to provide you with notice regarding a data security incident that has impacted the personal information of Idaho residents. Maximus provides this notice on behalf of applicable government agency customers (state and federal) in its capacity providing services in support of government programs as a contractor and, where applicable, business associate under the Health Insurance Portability and Accountability Act, Health Information Technology for Economic and Clinical Health Act, and their implementing regulations.

On May 30, 2023, Maximus detected unusual activity in MOVEit Transfer, a third-party software application provided by Progress Software Corporation ("Progress"), which is a tool used by Maximus to handle data transfers. Maximus promptly launched an investigation with the assistance of legal counsel and leading cybersecurity experts and quickly took its MOVEit Transfer environment offline. On May 31, 2023, Progress publicly announced a critical zero-day security vulnerability in the MOVEit Transfer software application. On June 12, 2023, the investigation revealed that as a result of this security vulnerability, an unauthorized party was able to copy files in Maximus' MOVEit Transfer environment that were maintained on behalf of certain federal and state government agencies in support of government programs. The investigation revealed that the files were copied between May 27, 2023 and May 31, 2023.

On or about July 19, 2023, Maximus' ongoing investigation revealed that the copied files may have contained the following types of personal information of at least 4,852 known Idaho residents: Name, address, telephone number, date of birth, individual taxpayer identification number (ITIN), social security numbers, contact information, health insurance information, government-issued identification card number, patient or plan number identifiers, and medical history information. The specific information impacted differed by individual depending on the government project at issue among other factors. Given the ongoing nature of the investigation, Maximus will provide supplemental information concerning material updates at the conclusion of its investigation, as appropriate.

Although the investigation determined the incident did not affect Maximus systems directly beyond Maximus' MOVEit Transfer environment, Maximus continues to enhance its cybersecurity posture to safeguard against ever evolving cyber threats, building on its written information security program. Upon initial detection, Maximus promptly launched an investigation, took its MOVEit Transfer environment offline, notified the impacted government agencies, and implemented vendor recommended security patches. Maximus also notified, and continues to cooperate with, the Federal Bureau of Investigation. Notification was not delayed as a result of a law enforcement investigation.

Maximus began notifying known affected Idaho residents via first class mail on July 28, 2023. Affected agencies have indicated that they will begin posting online notification regarding the incident and notifying news media on or about July 28, 2023. Enclosed is a sample notification letter being sent to affected individuals. Maximus has offered affected Idaho residents with 24 months of complementary IdentityWorks^{SM} credit monitoring, identity restoration, and fraud detection services, through Experian.

Maximus is also notifying the major consumer reporting agencies regarding the incident.

If you should have any questions, or if we can provide further assistance to the Idaho residents affected by this incident, please feel free to contact me.

Sincerely,

/s/ Paul Otto

Paul Otto
paul.otto@hoganlovells.com
(202) 637-5887

maximus

[DATE]

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

Name
Address 1
Address 2

Dear [Name]:

We are writing on behalf of Maximus Human Services, Inc. (Maximus) to notify you of an incident that involved unauthorized access to files which contain certain of your information. Maximus is a contractor to <<insert text>> (the "Agency") and provides services to support certain government programs, including <<insert text>>.

The incident involved an unauthorized party exploiting a vulnerability in MOVEit Transfer, a third-party software application provided by Progress Software Corporation (Progress), to gain access to files that contained some of your personal information. Maximus is among the many organizations in the United States and globally that have been impacted by the MOVEit vulnerability.

Your information was affected because it was transferred using the MOVEit application. We are providing this letter to help you understand what happened, what we are doing, and steps you can take to protect your information. Please read it carefully.

What happened?

On May 30, 2023, Maximus detected unusual activity in our MOVEit environment. Upon detection, Maximus promptly began to investigate with the help of nationally recognized cybersecurity experts. Early in the day on May 31, 2023, Maximus took its MOVEit application offline. Later that same day, Progress first publicly announced a previously unknown vulnerability in its MOVEit software, which an unauthorized party used to gain access to files of many MOVEit customers. Maximus subsequently applied vendor recommended actions, including applying new patches made available by Progress, to address the vulnerability.

Maximus promptly informed the Agency of the incident, and we have been working with them since. Additionally, we engaged a forensic investigation firm and a data analysis firm to identify affected individuals and the types of information involved. We learned that from approximately May 27th through May 31st, 2023, the unauthorized party obtained copies of certain files that were saved in the Maximus MOVEit application. Upon receiving this information, Maximus began to analyze the files to determine which data was affected. Our investigation determined that the files contained some of your personal information.

What information was involved?

The analysis has revealed that personal information involved in this breach varied by individual and may include: <<insert text>>. At this time Maximus has not identified evidence that data accessed has been improperly used.

What are we doing?

Maximus is offering two years of complimentary credit monitoring, identity restoration, and fraud detection services through Experian. If you would like to take advantage of the services that we are providing to you free of charge, please follow the instructions on Attachment 1.

Although the investigation has determined that the incident did not impact our systems directly, beyond our MOVEit environment, we continue to enhance our cybersecurity posture to safeguard against ever evolving cyber threats,

monitor for unusual activity and vulnerabilities, and apply vendor recommended actions as applicable. We also notified and are cooperating with law enforcement.

What can you do?

As good practice, it is recommended that you regularly monitor account statements and monitor free credit reports. If you identify suspicious activity, you should contact the company that maintains the account on your behalf. Additional information about how to protect your identity is contained in Attachment 2.

For more information:

Maximus takes the privacy and security of your personal information very seriously and regrets that this incident occurred.

If you have any questions or concerns, please contact us, toll-free, at 833-919-4749 Monday through Friday between 9:00 a.m. and 11:00 p.m. Eastern Standard Time, or Saturday and Sunday between 11:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding major U.S. holidays) and be prepared to provide your engagement number [B######].

Sincerely,

Maximus Privacy Office

Attachment 1: Credit Monitoring and Experian IdentityWorks℠ Membership Information

What you can do:
To help protect your identity, we are offering complimentary access to fraud detection and identity restoration services with Experian IdentityWorks℠ for 24 months.

If you believe there was fraudulent use of your information because of this incident and would like to discuss how you may be able to protect against those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by November 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: [Activation Code]

If you have questions about the product, need assistance with Identity Restoration that happened because of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **833-919-4749** by **November 30, 2023**. Be prepared to provide **engagement number [B######]** as proof of eligibility for the Identity Restoration services by Experian.

Additional details regarding your 24-month Experian IdentityWorks membership:

A credit card is not required for enrollment in Experian IdentityWorks. 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 file 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.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* 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.

Attachment 2: Additional Information

Below are additional helpful tips you may want to consider to protect your personal information.

It is good practice to remain vigilant by reviewing your financial statements and accounts for signs of suspicious transactions and activities. Report any indications of suspected fraud or identity theft to local law enforcement, your State's Attorney General's office, or the Federal Trade Commission ("FTC").

Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue NW Washington, DC 20580
1.877.FTC.HELP (382.4357) / www.ftc.gov/idtheft

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023.

For Kentucky residents: You may contact the Kentucky Office of the Attorney General, Office of Consumer Protection, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, www.ag.ky.gov, 1-855-813-6508.

For other residents, you may find information on how to contact your state attorney general by visiting https://www.naag.org/find-my-ag/.

Fraud Alert and Security Freeze Information

You may consider placing a free "Fraud Alert" on your credit file. Fraud Alerts tell potential credit grantors of possible fraudulent activity and to verify your identification before extending credit in your name. A Fraud Alert can make it more difficult for someone to get credit in your name, but also may delay your ability to obtain credit. Fraud alerts generally last one year. Identity theft victims can get an extended fraud alert for seven years.

Call only one of the following nationwide credit reporting companies to place your Fraud Alert. As soon as the credit reporting company confirms your Fraud Alert, they will forward your alert request to the other two nationwide credit reporting companies.

Equifax
PO Box 740256
Atlanta, GA 30374
www.equifax.com/personal/credit- report-services/credit-fraud-alerts/ 1-800-525-6285

TransUnion PO Box 2000
Chester, PA 19016
www.transunion.com/fraud
-alerts
1-800-680-7289

Experian PO Bo 9554
Allen, TX 75013
www.experian.com/fraud 1-888-397-3742

You also have the right to request a free Security Freeze (aka "Credit Freeze") on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. A Credit Freeze can make it more difficult for someone to get credit in your name, but also may delay your ability to obtain credit. You may also contact any of the credit reporting companies or the FTC for more information regarding Fraud Alerts and security freezes at:

Equifax Security Freeze PO Box 105788
Atlanta, GA 30348
http://www.equifax.com/personal/credit-report- services/credit-freeze/
1-800-349-9960

TransUnion Security Freeze
PO Box 2000
Chester, PA 19016
www.transunion.com/credit-freeze
1-888-909-8872

Experian Security Freeze
PO Box 9554
Allen, TX 75013
www.experian.com/freeze
1-888-397-3742