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

August 18, 2023

By Electronic Mail: *consumer@ag.iowa.gov*

The Honorable Brenna Bird
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Data Security Incident

Dear Attorney General Bird:

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 Iowa 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 August 13, 2023, Maximus' ongoing investigation revealed that the copied files may have contained the following types of personal information of at least 14,628 known Iowa residents: Name, address, date of birth, and social security number. 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 anticipates notifying these known affected Iowa residents via first class mail on August 25, 2023. Affected agencies have indicated that they will begin posting online notification regarding the incident and notifying news media on or about August 18, 2023. Enclosed is a sample notification letter being sent to affected individuals. Maximus has offered affected Iowa residents with 24 months of complementary IdentityWorks℠ 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 Iowa 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

Notice of Security Incident

Dear [Name]:

Maximus Health Services, Inc. (Maximus) writes to notify you of an incident that may involve some of your personal information. Maximus is a contractor to <<insert text>> (the "Department") and provides services to support certain government programs including <<insert text>>.

The incident involved a critical vulnerability in "MOVEit Transfer," a third-party computer software application provided by Progress Software Corporation (Progress). Maximus is among the many organizations in the United States and globally impacted by the MOVEit vulnerability.

We are sharing this to help you understand the incident, what we are doing to address it, and steps you can take to help protect your information.

What happened?

On May 30, 2023, Maximus detected unusual activity in our MOVEit environment. We promptly began to investigate and took the MOVEit environment offline early on May 31, 2023.

The investigation determined that from approximately May 27 to 31, 2023, an unauthorized party obtained copies of certain computer files saved in our MOVEit computer application. We promptly notified the Department of the incident. Following further review of these files, we determined that those files contained some of your personal information. We communicated this to the Department on <<insert text>>.

What information was involved?

The information involved may include your: <<insert text>>.

What are we doing?

As soon as we became aware of the incident, we took prompt action to investigate with the help of nationally recognized cybersecurity experts, took the MOVEit environment offline early on May 31, 2023, and applied vendor-recommended actions to address the previously unknown vulnerability. We continue to enhance our cybersecurity program to safeguard from cyber threats. We also notified and are cooperating with law enforcement.

What can you 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. You may also review the guidance contained in *Steps You Can Take to Protect Personal Information.*

maximus

As an added precaution, Maximus is offering you 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 review the enrollment instructions contained in the attachment.

For More Information.

We take the privacy and security of your personal information very seriously and regret that this incident occurred. If you have further questions or concerns or would like to enroll in free credit monitoring/ID theft protection by speaking to customer service, please call [Experian TFN] toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your **engagement number [B######]**.

Sincerely,

Maximus Privacy Office

Steps You Can Take To Protect Personal Information

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.