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

June 23, 2021

Wayne Stenehjem
North Dakota Attorney General
State Capitol, 600 E. Boulevard Ave., Dept. 125
Bismarck, ND 58505
ndag@nd.gov

By Email

Dear Attorney General Stenehjem,

I am writing on behalf of Maximus, Inc. to inform you of an incident that may have impacted personal information of North Dakota residents collected in connection with services that Maximus provides to the Ohio Department of Medicaid (ODM). Maximus partners with governments to provide communities with critical health and human service programs. Maximus is headquartered at 1891 Metro Center Drive, Reston, VA 20190.

On May 19, 2021, Maximus learned that a Maximus server that contained personal information provided to the ODM or to a Managed Care Plan for purposes of credentialing or tax identification of healthcare providers was accessed by an unknown party. We promptly isolated the server and engaged a leading digital forensics firm to assist with an investigation to determine the nature and scope of the incident. We determined that the server was impermissibly accessed between May 17 and 19, 2021. We have no indication that any personal information has been misused. Maximus has notified appropriate law enforcement, ODM, and the national credit reporting agencies regarding this incident.

Maximus has concluded that the incident impacted names, dates of birth, DEA numbers, and Social Security numbers. We have identified 319 North Dakota residents whose information was impacted by this incident. The total number of impacted individuals is 334,690.

Maximus has taken a number of steps to reduce the risks of this type of incident recurring, including isolating the affected server, engaging a leading digital forensics firm to investigate, and reviewing its existing server configurations and security processes.

Maximus sent notice by mail to the impacted North Dakota residents on Friday, June 18, 2021. We include a sample notice in this notification. In addition to providing information regarding credit reporting agencies, state attorneys general offices, security freezes, fraud alerts, and other identity theft protection tools, Maximus is offering credit monitoring and identity protection services for two years through Experian, at no cost to the impacted individuals.

Please feel free to contact me if you have any questions or require additional information.

Sincerely,

/s/ Allison M. Holt Ryan

Allison M. Holt Ryan

Partner
allison.holt-ryan@hoganlovells.com

MAXIMUS®
Important Information for
Ohio Medicaid Providers
Return Mail Processing
PO Box 999
Suwanee, GA 30024

1057 1 334667 **********AUTO**ALL FOR AADC 980
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

June 18, 2021

NOTICE OF DATA BREACH

Dear Sample A. Sample,

Maximus is writing to tell you that we recently experienced a cybersecurity incident where an actor accessed a Maximus server that involved personal information that we received in connection with services that Maximus provides.

What Happened

On May 19, 2021, Maximus learned that a Maximus server that contained personal information provided to the Ohio Department of Medicaid (ODM) or to a Managed Care Plan for purposes of credentialing or tax identification in your role as a healthcare provider was accessed by an unknown party. We promptly isolated the server. We engaged a leading digital forensics firm to assist with an investigation to determine the nature and scope of the incident. The investigation determined that the server was impermissibly accessed starting on May 17, 2021. We have no indication that your information has been misused, but in an abundance of caution, we are informing you so that you may take precautionary measures. Maximus also notified appropriate law enforcement and ODM.

What Information Was Involved

The information that may have been accessed includes your name, date of birth, Social Security number, and DEA number.

What We Are Doing

We have taken several steps to reduce the risk of this type of incident recurring. We identified how the incident happened and made changes so it should not happen again. We also have arranged for you to obtain, at no cost to you, 24 months of credit monitoring and other services from Experian. Information regarding the package of services is included in Attachment 1 to this letter. We also want you to know about other protective actions you can take.

What You Can Do

We are not aware of any evidence indicating that your personal information has been sold or is being misused. However, we recommend that you remain vigilant by reviewing your account statements and monitoring your free credit reports for signs of suspicious activity. Please find additional information in Attachment 2 to this letter. As noted above, you can enroll, at no cost to you, in 24 months of credit monitoring and other services from Experian. Those services include ongoing monitoring of your personal information for possible misuse. Information about enrollment is included with this letter.

For More Information

If you have any questions or need additional information, please contact (800) 357-0823 Monday to Friday 9:00 AM – 11:00 PM EDT and Saturday to Sunday 11:00 AM – 8:00 PM EDT by September 30, 2021.

We apologize for any inconvenience this may cause.

Sincerely,

Ira J. Rothman
Senior Vice President – Privacy Official

Attachment 1: Credit Monitoring and Identity Theft Services Enrollment Information

What we are doing to protect your information:

To help protect your identity, we are offering a complimentary 24 month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **September 30, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bplus
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (800) 354-0823 by **September 30, 2021.** Be prepared to provide engagement number **B014394** 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, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **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.
- **Up to $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.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (800) 354-0823. 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 (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 this Identity Restoration support 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. You will also find self-help tips and information about identity protection at this site.

Attachment 2: Additional Information

You should be cautious about using email to provide sensitive personal information, whether sending it yourself or in response to email requests. You should also be cautious when opening attachments and clicking on links in emails. Scammers sometimes use fraudulent emails or other communications to deploy malicious software on your devices or to trick you into sharing valuable personal information, such as account numbers, Social Security numbers, or usernames and passwords. The Federal Trade Commission (FTC) has provided guidance at https://www.consumer.ftc. gov/articles/0003-phishing.

You should review your financial statements and accounts for signs of suspicious transactions and activities. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to local law enforcement, your State's Attorney General's office, or the FTC. You will find contact information for some of those entities below. If you discover unauthorized charges, promptly inform the relevant payment card companies and financial institutions.

Fraud Alert Information

Whether or not you enroll in the credit monitoring product offered, we recommend that you consider placing a free "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Fraud alerts last one year. Identity theft victims can get an extended fraud alert for seven years.

Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. You may also contact any of the consumer reporting agencies or the FTC for more information regarding Fraud Alerts. The contact information for the three nationwide credit reporting companies is:

Equifax	TransUnion	Experian
PO Box 740256	PO Box 2000	PO Box 9554
Atlanta, GA 30374	Chester, PA 19016	Allen, TX 75013
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/	www.transunion.com/fraud	www.experian.com/fraud
1-800-525-6285	1-800-680-7289	1-888-397-3742

Free Credit Report Information

You have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in your credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score. Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, we recommend that you check your account statements and credit reports periodically. You should remain vigilant for incidents of fraud and identity theft. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency or state attorney general and file a police report. Get a copy of the report; many creditors want the information it contains to alleviate you of the fraudulent debts. You also should file a complaint with the FTC using the contact information below. Your complaint will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcement for their investigations.

You may also contact the FTC at the contact information below to learn more about identity theft and the steps you can take to protect yourself and prevent such activity. If you are a resident of the District of Columbia, Iowa, Maryland, New York, or Oregon, you can also reach out to your respective state's Attorney General's office at the contact information below. All other residents can find information on how to contact your state attorney general at https://www.naag.org/find-my-ag/.

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

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, DC 20001
1-202-727-3400 / oag.dc.gov

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
1-877-877-9392 / https://justice.oregon.gov

Maryland Attorney General's Office
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023 / www.marylandattorneygeneral.gov

New York Attorney General's Office
The Capitol
Albany, NY 12224-0341
1-800-771-7755
https://ag.ny.gov/consumer-frauds-bureau/identity-theft

Consumer Protection Division
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319
1-515-281-5926 / www.iowaattorneygeneral.gov

Security Freeze Information

You 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. When a Credit Freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A Credit Freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. You may also contact any of the consumer reporting agencies or the FTC for more information regarding Security Freezes.

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/freeze
1-888-909-8872

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

To request a Credit Freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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.)

New Mexico residents: You have the right to obtain a Credit Freeze or submit a declaration of removal under the New Mexico Fair Credit Reporting and Identity Security Act. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the New Mexico Fair Credit Reporting and Identity Security Act.