Lindsay B. Nickle
Partner, Vice Chair
1201 Elm Street, Suite 2550
Dallas, Texas 75270
LNickle@constangy.com
Direct: 806.535.0274

July 15, 2024

VIA EMAIL
Attorney General Brenna Bird
Office of the Attorney General
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, IA 50319
consumer@ag.iowa.gov

Re: Notice of Data Security Incident

Dear Attorney General Bird:

Constangy Brooks Smith & Prophete LLP represents MNGI Digestive Health ("MNGI") in connection with a recent data security incident described in greater detail below.

1. **Nature of the security Incident.**

On August 25, 2023, MNGI discovered unauthorized activity within its digital environment. In response, MNGI took steps to secure its network and began an investigation. MNGI also engaged independent cybersecurity experts to assist with the investigative efforts. This investigation determined that unauthorized access to certain portions of its network occurred on August 20, 2023. Following a thorough and time-intensive review of the affected data, MNGI learned on June 7, 2024 that certain individuals' personal and protected health information was potentially affected by this incident. Since that time, MNGI has been diligently collecting up-to-date address information needed to notify all potentially affected individuals.

Please note that MNGI has no evidence of the misuse or attempted misuse of any potentially impacted information.

The information that may have been accessible by the malicious actor(s) responsible for this incident varies by individual and may include individuals' names, medical information, health insurance information, dates of birth, patient account numbers, financial account information, driver's license or state ID numbers, passport numbers, payment card information, usernames and associated passwords, taxpayer ID numbers, biometric data, and/or Social Security numbers.

2. **Number of Iowa residents affected.**

MNGI began notifying 711 Iowa residents of this incident via first class U.S. mail on July 15, 2024, and completed the notification on July 17, 2024. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as MNGI learned of this incident, MNGI took steps to evaluate the potentially affected data and determine whether any personal or protected health information was affected.

MNGI has also established a toll-free call center through Epiq, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. The call center is available at 1- 888-326-0965 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays). In addition, while MGNI is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, MNGI is also providing complimentary identity protection services to notified individuals whose Social Security numbers may have been affected by the incident.

4. Contact information.

MNGI remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me.

Best regards,

Lindsay B. Nickle
Partner

Enclosure: Sample Notification Letter

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

To Enroll, Please Call:

866.622.9303

Or Visit:

app.identitydefense.com/enrollment/activate/mngi

Enrollment Code: <<Activation Code>>

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Subject: Notice of Data <<Variable Header>>

Dear <<Full Name>>,

We are writing to inform you about a recent data security incident experienced by MNGI Digestive Health ("MNGI"), headquartered in Minneapolis, Minnesota, that may have affected your personal and protected health information. MNGI takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your information.

What Happened? On August 25, 2023, MNGI discovered unauthorized activity within its digital environment. In response, MNGI took steps to secure its network and began an investigation. MNGI also engaged independent cybersecurity experts to assist with the investigative efforts. This investigation determined that unauthorized access to certain portions of our network occurred on August 20, 2023. Following a thorough and time-intensive review of the affected data, MNGI learned on June 7, 2024 that your personal and protected health information was potentially affected by this incident. Please note that MNGI has no evidence of the misuse or attempted misuse of any potentially impacted information.

What Information Was Involved? The information potentially impacted in connection with this incident included your name and <<Data Elements>>.

What Are We Doing? As soon as MNGI discovered this incident, it took the steps described above. In addition, MNGI has implemented measures to enhance the security of its digital environment in an effort to minimize the risk of a similar incident occurring in the future.

Although MNGI has no evidence of the misuse of any potentially impacted information, MNGI is providing you with information about steps that you can take to help protect your personal and protected health information and offering you complimentary <<CM Duration>> months of identity protection services through CyEx – a data breach and recovery services expert. The deadline to enroll in these services is **<<Enrollment Deadline>>**.

What You Can Do: You can follow the recommendations on the following page to help protect your personal and protected health information. MNGI also encourages you to enroll in the complimentary services offered to you through CyEx by using the enrollment code noted above.

For More Information: Further information about how to protect your personal and protected health information appears on the following page. If you have questions or need assistance, please call 888-326-0965 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays). Call center representatives are fully versed on this incident and can answer any questions that you may have.

Please accept my sincere apologies and know that MNGI takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

MNGI Digestive Health
P.O. Box 14909
Minneapolis, MN 55414

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

Rhode Island: The total number of individuals receiving notification of this incident is <<# of Notice Sent>>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.