LEWIS BRISBOIS BISGAARD & SMITH LLP

Maria Efaplomatidis
77 Water Street, Suite 2100
New York, NY 10005
Maria.Efaplomatidis@lewisbrisbois.com
Direct: 212.232.1366

December 20, 2022

VIA ELECTRONIC MAIL

Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 033
Email: DOJ-CPB@doj.nh.gov

Re: **Notice of Data Security Incident**

Dear Attorney General Formella:

Lewis Brisbois Bisgaard & Smith LLP represents Heartland Alliance ("Heartland") in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with New Hampshire's data breach notification statute.

1. Nature of the Incident

In late January 2022, Heartland experienced a disruption to its digital environment. Upon discovering this access, Heartland immediately took steps to secure the environment and investigate. It also engaged independent cybersecurity experts to conduct an investigation. As a result of this investigation, Heartland learned on April 27, 2022, that an unauthorized actor may have accessed certain personal information stored within its system. Since then, Heartland has been working diligently to obtain contact information for all individuals that may have been impacted by the incident. Heartland completed its work to obtain the necessary group designation and corresponding contact information by November 30, 2022. These individuals whose address information was available were notified via U.S. First-Class Mail beginning on December 15, 2022. Additionally, Heartland posted notice of the data security incident on the home page of its website, which will remain for a period of at least ninety (90) days.

The information affected varies by individual but may include individuals' names, date of birth, Social Security numbers, driver's license numbers, financial account numbers, and/or certain health

or medical information. To date, Heartland has no evidence that any potentially impacted information has been misused in conjunction with the incident.

2. **Number of New Hampshire Residents Involved**

On December 15, 2022, Heartland notified two (2) New Hampshire residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence. Please note that the impacted data elements vary between individuals, depending on the type of association each individual had with Heartland (e.g. employee, health participant, independent contractor, etc.).

3. Steps Taken to Address the Incident

To help prevent something like this from happening again, Heartland is implementing additional technical security measures. Heartland is also providing individuals with information about steps that they can take to help protect their personal information, and, out of an abundance of caution, it is also offering individuals complimentary credit monitoring and identity protection services through IDX.

4. Contact Information

Heartland 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 at 212.232.1366 or Maria.Efaplomatidis@lewisbrisbois.com.

Sincerely,

Maria Efaplomatidis of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

Enclosure: Sample Notification Letter

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

To Enroll, Please Call:
(833) 896-6542
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<Enrollment Code>>

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

December 15, 2022

Re: Notice of Data <<Variable 1>>

Dear <<First Name>> <<Last Name>>,

I am writing about a data security incident experienced by Heartland Alliance ("Heartland") that may have involved your personal information.

We have no evidence to suggest misuse or even attempted misuse of your information. To be as careful as possible, however, we are notifying you of this incident and offering you free credit monitoring and identity protection services. This letter explains what happened and what you should do if you want to sign up for credit monitoring and identity protection services at no cost to you.

Heartland takes this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this incident may cause you.

What Happened. In late January, 2022, Heartland learned of suspicious activity in our IT system. We immediately secured the system and hired a leading cybersecurity firm to investigate. Through the investigation, on April 27, 2022, we found that an unauthorized individual may have accessed personal information in our system. Since then, we have been working to determine what information may have been accessed and to gather contact information so that we could notify all potentially affected current and former employees and participants. We completed our work to obtain the necessary employee contact information on November 22, 2022.

What Information Was Involved. The information that may potentially have been accessed includes your name, Social Security number, driver's license number, bank account number, and date of birth. No medical or health insurance information was accessed.

What We Are Doing. As soon as we discovered this incident, we took the steps described above. We also added new security features to our IT systems to reduce the risk of something like this happening again. In addition, we reported the incident to the Federal Bureau of Investigation and will cooperate with any resulting investigation.

What You Can Do. While the investigation did not find any evidence to suggest your information has been misused, we recommend that you take the following steps:

First, enroll in the free credit monitoring and identity protection services Heartland is offering through a company called IDX. These services include: <<12/24 Months>> of credit and dark web monitoring, assistance with identity theft recovery if you are the victim of identity theft, and an insurance policy to cover any identity recovery costs.

You may sign up for these services, without any cost to you, by calling (833) 896-6542 or going to https://app.idx.us/account-creation/protect and using the enrollment code provided above. Representatives are available from 8:00am to 8:00pm Central Time from Monday to Friday. Spanish-speaking agents will be available. **Please note the deadline to enroll is March 15, 2023.**

Second, we recommend that you review the guidance included with this letter about additional steps you can take to protect your personal information.

For More Information. If you have questions or need assistance, please contact IDX at (833) 896-6542, Monday through Friday from 8:00am to 8:00pm Central Time, excluding major U.S. holidays. Representatives are fully informed about this incident and can answer any questions you may have.

We are committed to protecting your personal information and deeply regret that this incident occurred.

Sincerely,

Kelli Spencer
Privacy Officer
Heartland Alliance

208 S. LaSalle Street
Suite 1300
Chicago, IL 60604

Steps You Can Take to Protect Your Personal 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 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-800-831-5614
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
1-877-438-4338

Maryland Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

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
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

Illinois Attorney General
100 West Randolph Street
Chicago, IL 60601
illinoisattorneygeneral.gov
1-312-814-3000

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://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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

To Enroll, Please Call:
(833) 896-6542
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

December 21, 2022

Re: Notice of Data <<Variable Text 1>>

Dear <<FIRST NAME>> <<LAST NAME>>,

I am writing about a data security incident experienced by Heartland Alliance ("Heartland"). This incident may have involved your personal information because Heartland Alliance Health, which has provided you with health care services, keeps some of its records on Heartland's IT system.

We have no evidence to suggest misuse or even attempted misuse of your information, but we take the privacy and security of your information very seriously. To be as careful as possible, we are notifying you of this incident and offering you free credit monitoring and identity protection services. This letter explains what happened and what you should do if you want to sign up for credit monitoring and identity protection services at no cost to you.

Heartland takes this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this incident may cause you.

What Happened. In late January 2022, Heartland learned of suspicious activity in our IT system. We immediately secured the system and hired a leading cybersecurity firm to investigate. Through the investigation, on April 27, 2022, we found that an unauthorized individual may have accessed personal information in our system. Since then, we have been working to determine what information may have been accessed and to gather contact information so that we could notify all potentially affected Heartland Alliance Health participants. We completed our work to obtain the necessary contact information on November 17, 2022.

What Information Was Involved. This incident did not involve our electronic medical record system that contains your entire record. The potentially affected information may have included your name, Social Security number, date of birth, some pieces of medical or health information such as diagnosis, medication and medication monitoring notes, other health care provider and case manager notes, and, for dental patients, dental scans.

What We Are Doing. As soon as we discovered this incident, we took the steps described above. We also added new security features to our IT systems to reduce the risk of something like this happening again. In addition, we reported the incident to the Federal Bureau of Investigation and will cooperate with any resulting investigation.

What You Can Do. While the investigation did not find any evidence to suggest that your information has been misused, we recommend that you take the following steps:

First, enroll in the free identity protection services Heartland is offering through a company called IDX. These identity protection services include: <<12/24 months>> of credit and dark web monitoring, assistance with identity theft recovery if you are the victim of identity theft, and an insurance policy to cover any identity recovery costs.

You may sign up for these services, without any cost to you, by calling (833) 896-6542 or going to https://app.idx.us/account-creation/protect and using the enrollment code provided above. Representatives are available from 8:00am to 8:00pm Central Time from Monday to Friday. Spanish-speaking agents will be available. **Please note the deadline to enroll is March 21, 2023.**

Second, we recommend that you review the guidance included with this letter about additional steps you can take to protect your personal information.

For More Information. If you have questions or need assistance, please contact IDX at (833) 896-6542, Monday through Friday from 8:00am to 8:00pm Central Time, excluding major U.S. holidays. Representatives are fully informed about this incident and can answer any questions you may have.

We are committed to protecting your personal information and deeply regret that this incident occurred.

Sincerely,

Kelli Spencer
Privacy Officer
Heartland Alliance

208 S. LaSalle Street
Suite 1300
Chicago, IL 60604

Steps You Can Take to Protect Your Personal 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 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-800-831-5614
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
1-877-438-4338

Maryland Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

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
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

Illinois Attorney General
100 West Randolph Street
Chicago, IL 60601
illinoisattorneygeneral.gov
1-312-814-3000

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://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.