CONSTANGY BROOKS, SMITH & PROPHETE LLP

April 26, 2024

VIA EMAIL
Attorney General John M. Formella
Office of the Attorney General
Consumer Protection & Antitrust Bureau
1 Granite Place South
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: **Notice of Data Security Incident**

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP ("Constangy") represents South Shore Mental Health d/b/a Aspire Health Alliance ("Aspire Health") in connection with the data security incident described below.

Nature of the Security Incident

On September 13, 2023, Aspire Health discovered unusual activity in its digital environment. Upon discovering this activity, Aspire Health immediately took steps to secure its network and launched an investigation, aided by independent cybersecurity experts, to determine what happened and whether sensitive information may have been affected. As a result of the investigation, Aspire Health learned that an unauthorized actor acquired certain files and data stored within its systems. Following a comprehensive review of the impacted data, which concluded on February 26, 2024, Aspire Health determined that individuals' personal and / or protected health information may have been impacted, and moved as quickly as possible to provide notice and resources to assist.

The information that was potentially impacted in this incident varies by individual but may include . Aspire Health has no evidence of any actual or attempted misuse of this information.

Number of New Hampshire Residents Involved

On April 26, 2024, Aspire Health will be notifying thirty-eight (38) New Hampshire residents of this incident via U.S. First-Class Mail. A sample copy of the notification letter being sent to impacted individuals is included with this correspondence.

Steps Taken to Address the Incident

Aspire Health has implemented additional security measures in its environment to reduce the risk of a similar incident occurring in the future. Aspire Health also reported the incident to the Federal Bureau of Investigation and is cooperating with its investigation. In addition, out of an abundance of caution, Aspire Health is providing complimentary credit monitoring and identity protection services to individuals whose were impacted, along with additional resources to assist. Aspire Health has also established a toll-free call center to address any questions and to help individuals resolve issues if their identity is compromised due to this incident.

Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at .

Sincerely,

David McMillan of
Constangy, Brooks, Smith & Prophete, LLP

Enclosure: Sample Notification Letter

aspire health alliance

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

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

April 26, 2024

Subject: Notice of Data <<Variable Text 1 – Breach or Security Incident>>:

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

We write to inform you of a recent data security incident experienced by Aspire Health Alliance ("Aspire Health") that may have affected some of your information. Please read this letter carefully as it contains details about the incident and resources you may utilize to help protect your information.

What Happened? On September 13, 2023, we discovered unusual activity in our digital environment. Upon discovering this activity, we immediately took steps to secure the network and launched an investigation, aided by independent cybersecurity experts, to determine what happened and whether sensitive information may have been affected. As a result of the investigation, we learned that an unauthorized actor acquired certain files and data stored within our systems. We then launched a comprehensive review of the potentially affected files to identify any personal or protected health information that may have been impacted. Our review concluded on February 26, 2024 and confirmed that your personal and / or protected health information was included within the impacted files. We then worked diligently to identify up-to-date mailing addresses in order to provide notice to potentially impacted individuals.

What Information Was Involved? The information that was potentially impacted in connection with this incident includes your Please note that we have no evidence of any actual or attempted misuse of this information.

What Are We Doing? As soon as Aspire Health discovered the incident, Aspire Health took immediate steps to secure its environment and enlisted a leading, independent cybersecurity firm to conduct a forensic investigation. Aspire Health also reported the incident to the FBI and will cooperate with any resulting investigation. In addition, we have implemented several measures to enhance our network security and reduce the risk of similar future incidents.

Furthermore, to help relieve concerns and restore confidence following this incident, Aspire Health is providing you with the opportunity to enroll in complimentary credit monitoring and identity theft protection services through IDX – a data breach and recovery services expert. These services include: of credit[1] and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. To enroll, please visit and provide the Enrollment Code above. With this protection, IDX will help you resolve issues if your identity is compromised. Please note that the deadline to enroll is

What You Can Do: Aspire Health recommends that you review the guidance included with this letter about how to help protect your information. We also encourage you to enroll in the credit monitoring and identity protection services we are offering, which are at no cost to you.

For more information. If you have any questions about this incident or the complimentary services being offered, please contact our dedicated call center at 1-888-714-9989, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays. Please have your enrollment code ready.

We take the privacy and security of all information within our possession very seriously. Please accept our sincere apologies and know that Aspire Health deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Aspire Health Alliance
1501 Washington St.
Braintree, MA 02184

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

Massachusetts Attorney General
1 Ashburton Place, Suite 1801
Boston, MA 02108
https://www.mass.gov/orgs/office-of-the-attorney-general
1-617-727-2200

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.