

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: (410) 456-2741
Cell: (410) 917-5189
E-mail: spollock@mcdonaldhopkins.com

July 19, 2024

VIA EMAIL: Idtheft@oag.state.md.us

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Arisa Health Inc. – Incident Notification

Dear Sir or Madam:

McDonald Hopkins represents Arisa Health. I am writing to provide notification of an incident that may affect the security of personal information of approximately one (1) Maryland resident. By providing notice, Arisa Health does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about March 18, 2024, Arisa Health experienced a cybersecurity incident that impacted connectivity to its network. Upon learning of this issue, Arisa Health immediately commenced a prompt and thorough investigation. As part of its investigation, Arisa Health has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual review, on May 20, 2024 Arisa Health confirmed that between March 1, 2024 and March 18, 2024, certain impacted files containing personal information may have been subject to unauthorized access or acquisition. The potentially impacted information includes full name, and Social Security Number.

Arisa Health has no reason to believe that any personal information will be misused as a result of this incident. Nevertheless, out of an abundance of caution, Arisa Health wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Arisa Health is providing the affected resident with written notification of this incident commencing on or about July 19, 2024 in substantially the same form as the letter attached hereto. Arisa Health is also offering the affected residents a complimentary one-year membership with a credit monitoring service. Arisa Health is advising the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Arisa Health is advising the affected resident about the process for placing fraud alerts and/or security freezes on their credit file and obtaining

July 19, 2024

Page 2

a free credit report. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Arisa Health, protecting the privacy of personal information is a top priority. Arisa Health is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Arisa Health continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

If you have any additional questions, please contact me at (410) 456-2741 or spollock@mcdonaldhopkins.com.

Sincerely Yours,

A handwritten signature in blue ink, appearing to read "Spencer S. Pollock".

Spencer S. Pollock, Esq., CIPP/US, CIPM

Encl.

Arisa Health Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



July 19, 2024

Important Information Please Review Carefully

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Arisa Health Incorporated ("Arisa Health"). Please note, Arisa Health has multiple subsidiaries, including Counseling Associates, Inc., Northeast Arkansas Community Mental Health Center d/b/a Mid-South Health Systems, Ozark Guidance Center, Inc., and Professional Counseling Associates, Inc. We are writing with important information regarding a data security incident. As such, we want to provide you with information about the incident, tell you about the services that we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On or about March 18, 2024, Arisa Health experienced a cybersecurity incident that impacted connectivity to our network.

What We Are Doing

Upon learning of this issue, we immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and comprehensive document review, on May 20, 2024, we determined your personal data may have been subject to unauthorized access or acquisition, which occurred between March 1, 2024 and March 18, 2024.

What Information Was Involved?

The information potentially impacted includes your [REDACTED]

What You Can Do

We have no evidence that any of your information has been misused. To protect you from potential misuse of your information, we are offering a complimentary twelve (12)-month membership of Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

000010103G0400

P

For More Information

Attached to this letter, please review the “Other Important Information” document which provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

Arisa Health is committed to maintaining the privacy of personal information in our possession and has taken many precautions to safeguard it. Arisa Health continually evaluates and modifies its practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED] This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against potential misuse of your minor’s information. The response line is available 8:00am to 8:00pm ET, Monday through Friday, excluding holidays.

Sincerely,

Arisa Health Incorporated
2400 S 48th St
Springdale, Arkansas 72762, US

- OTHER IMPORTANT INFORMATION -

1. **Enrolling in Complimentary twelve (12)-Month Credit Monitoring.**

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services:
[REDACTED]

In order for you to receive the monitoring services described above, **you must enroll within 90 days from the date of this letter.** The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.



2. **Obtain and Monitor Your Credit Report**

Under federal law, you are entitled to one free credit report every 12 months from each of the three major nationwide credit reporting companies. You can obtain a free copy of your credit report by calling **1-877-322-8228**, visiting **www.annualcreditreport.com**, 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 can access the request form at <https://www.annualcreditreport.com/index.action>. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below.

00001020380000

P

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013

<https://www.experian.com/fraud-center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000

Chester, PA 19016-2000
<https://www.transunion.com/fraud-alert>
S
(800) 680-7289

Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

3. **Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013

<https://www.experian.com/fraud-center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000

Chester, PA 19016-2000
<https://www.transunion.com/fraud-alert>
S
(800) 680-7289

4. Placing a Security Freeze on Your Credit File.

Following is general information about how to request a security freeze from the three credit reporting agencies at no charge. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below). You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013

<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094

<https://www.transunion.com/credit-freeze>
eze
(888) 909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report 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 and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

