



Laura Funk, Partner
Cybersecurity & Data Privacy Team
1201 Elm Street, Ste 2550
Dallas, TX 75270
Telephone: 248.709.9385
Email: lfunk@constangy.com

January 19, 2024

VIA EMAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Re: **Notice of Data Security Incident**

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP (“Constangy”) represents Aria Care Partners (“Aria”), in connection with a data security incident described in greater detail below. Aria hereby reserves all rights and defenses in connection herewith.

Nature of the Security Incident

On May 12, 2023, Aria became aware of unusual activity that disrupted access to its vision file server. Upon discovering this activity, Aria immediately took steps to secure its network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened. Based on that investigation, Aria learned that an unknown actor gained unauthorized access to the Aria network and may have acquired certain files, some of which may have contained individuals’ personal and/or protected health information. Aria undertook a comprehensive review of the potentially impacted data to identify the individuals and information involved, which concluded on December 20, 2023.

Please note that Aria has no current evidence to suggest misuse or attempted misuse of personal information involved.

Number of Affected Maryland Residents & Information Involved

The incident involved personal information for approximately twenty-four (24) Maryland residents. The information involved in the incident may differ depending on the individual but may include the following for affected Maryland residents: name, Social Security number, medical information, and health insurance information.

Notification of Affected Individuals

On January 19, 2024, notification letters were mailed to affected Maryland residents by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers 12 months of complimentary identity protection services to each individual whose personal information was affected by this event, including credit monitoring, \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. Those services are offered by IDX, a company specializing in fraud assistance and remediation services. IDX will also support a call center for 90 days to answer questions and assist with enrollment. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

Steps Taken to Address the Incident

In response to the incident, Aria retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. Aria also implemented additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future. Additionally, Aria has reported the incident to the FBI and will cooperate with any resulting investigation.

Finally, Aria is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above.

Contact Information

Aria 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 LFunk@constangy.com or 248.709.9385.

Sincerely,

A handwritten signature in black ink, appearing to read 'L. Funk', with a long, sweeping horizontal line extending to the right.

Laura Funk of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Consumer Notification Letter

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

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:
<https://app.idx.us/account-creation/protect>

January 19, 2024

Subject: Notice of Data <<Variable 1>>

Dear <<First Name>> <<Last Name>>:

We are writing to inform you about a recent data security incident experienced by Aria Care Partners (“Aria”) that may have involved your personal and / or protected health information. Aria takes the privacy and security of all information within its possession very seriously. That is why we are writing to notify you of the incident, offer you complimentary credit monitoring and identity protection services, and provide you with information about steps you can take to help protect your information.

What Happened? On May 12, 2023, Aria detected unusual activity within our vision file server. Upon discovery, we immediately took steps to secure our network and engaged a leading, independent digital forensics and incident response firm to investigate what happened and whether any sensitive data may have been impacted. Based on that investigation, Aria learned that an unknown actor gained unauthorized access to our network and may have acquired certain files, some of which may have contained individuals’ personal and / or protected health information. Aria undertook a comprehensive review of the potentially impacted data to identify the individuals and information involved, which concluded on December 20, 2023. Aria then worked diligently to provide notification as soon as possible.

What Information Was Involved? The information that was potentially impacted during this incident may have included your name, as well as your <<Variable 2>>. Please note that Aria is not aware of any attempted or actual misuse of this information.

What Are We Doing? As soon as Aria discovered the incident, we took the steps described above and implemented measures to enhance the security of our network and reduce the risk of a similar incident occurring in the future. Aria also reported the incident to the Federal Bureau of Investigation and is cooperating with any resulting investigation to hold the perpetrator(s) accountable.

While we have no evidence that any of your information was misused, out of an abundance of caution, we are also offering you the ability to enroll in <<12/24>> months of complimentary credit monitoring and identity protection services through IDX, a national leader in identity protection services. The IDX services, which are free to you upon enrollment, include a <<12/24>> month subscription for the following: credit monitoring,¹ CyberScan dark web monitoring, fully managed identity recovery services, and \$1 million in identity theft insurance coverage. With this protection, IDX will help you resolve issues if your identity is compromised.

¹ To receive credit monitoring services, you must be over the age of 18 and have established credit in the United States, have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

What Can You Do? You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the IDX identity protection services, which are offered to you at no cost.

To enroll, please call 1-888-904-8810 or visit <https://app.idx.us/account-creation/protect> and provide the enrollment code at the top of this page. Please note you must enroll by April 19, 2024. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

For More Information: If you have questions or need assistance, please contact 1-888-904-8810 Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Sincerely,

John Rosenbaum

John Rosenbaum
Chief Compliance Officer
Aria Care Partners
8500 West 110th Street, Suite 260
Overland Park, KS 66210

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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the FTC is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

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 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 can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 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 Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. 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>. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the FTC identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

Oregon: Oregon Office of the Attorney General can be reached at: Oregon Department of Justice, 1162 Court St. NE, Salem, OR, 97301, 1-877-877-9392, www.doj.state.or.us

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>. The total number of Rhode Island residents receiving notification of this incident is <<XX>>.

Texas: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov