

Morgan Lewis

Gregory T. Parks

Partner
215.963.5170
gregory.parks@morganlewis.com

February 27, 2025

VIA EMAIL TO IDTHEFT@OAG.STATE.MD.US

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

Re: Notice of Data Security Incident

Dear Office of the Attorney General:

This Firm represents Aya Healthcare, Inc. ("Aya"), a provider of healthcare staffing services, and we are writing to notify your office about the nature and circumstances of a recent data security incident. Pursuant to applicable law, Aya is sending notice to 76 Maryland residents on February 27, 2025.

On January 29, 2025, Aya identified certain individuals whose personal information had been exposed in a credential stuffing incident. Through this credential stuffing incident, unauthorized third parties used lists of credentials (usernames and passwords) to attempt to gain access to Aya's systems. Notably, these credentials were not obtained from Aya. Rather, the credentials were obtained from unrelated sources or websites where individuals likely used the same username and password. A small number of the attempts to gain access to Aya's systems were successful, resulting in what we believe to be an automated bot logging into Aya's systems and viewing certain limited information associated with user accounts.

The impacted individuals had provided personal information to Aya in connection with their applications for travel or other temporary nursing positions. Through its investigation, Aya determined that the impacted information potentially included first names, last names, addresses, email addresses, phone numbers, dates of birth, state nursing license numbers, Social Security numbers, and/or vaccination status. There is no indication that the impacted information was viewed or downloaded by any person. Rather, it appears the information was only accessed by an automated bot agent.

Although there is no indication that the impacted personal information has been used for any fraudulent purpose, notifications are being sent by mail to the affected individuals to explain what happened, what information was involved, what has been done, and how affected individuals can contact Aya for more information. Two years of free credit monitoring are being offered to affected individuals whose Social Security numbers were impacted.

Morgan, Lewis & Bockius LLP

2222 Market Street
Philadelphia, PA 19103-3007
United States

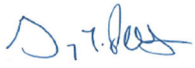
T +1.215.963.5000
F +1.215.963.5001

State of Maryland
Office of the Attorney General
February 27, 2025
Page 2

Upon initial detection of the unauthorized activity, Aya immediately took containment steps and commenced an investigation with the assistance of cybersecurity experts. Aya also reset the passwords of impacted individuals so that the password that the unauthorized third parties obtained from some other source would no longer enable access to their Aya accounts. Aya is also providing suggestions and reminders to affected individuals to use unique passwords that they do not use with other services.

Further information about what mitigations have been completed to date and what further mitigations are recommended to affected individuals can be found in the enclosed individual notification that Aya is sending via mail on February 27, 2025.

Regards,

A handwritten signature in blue ink, appearing to read "G. T. Parks", is written above the printed name.

Gregory T. Parks

Enclosure

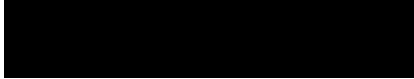


Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

February 27, 2025



M8894-L01-0000399 P001 T00002 *****MIXED AADC 159



Re: Notice of Data Security Incident

Dear 

We are writing to notify you of the potential exposure of your personal information in a recent data security incident at Aya Healthcare, Inc. ("Aya"). There is no indication that your personal information was misused in any way that could cause harm to you, but we are sending this letter to tell you what happened, what information was potentially involved, what we have done and what you can do to address this situation. Please read this letter carefully.

What Happened?

On January 12 and 19, 2025, Aya learned that unauthorized third parties were attempting to use lists of credentials (usernames and passwords) to attempt to gain access to user accounts on Aya's systems. Notably, these credentials were not obtained from Aya. Rather, the credentials were obtained from unrelated sources or websites where you likely used the same username and password. Using the same username and password across multiple websites is not recommended as it can make it easier for unauthorized third-parties to gain access to your accounts. A small number of the attempts to gain access to Aya's systems were successful, resulting in what we believe to be an automated bot logging into Aya's systems and viewing certain limited information. On January 29, 2025, Aya confirmed that your account was accessed in this manner using a password obtained from an unrelated source.

What Information Was Involved?

The impacted information included certain information that you provided to Aya in connection with your potential or actual Aya assignments, including your first name, last name, phone number, email address, state nursing license number, address, date of birth, Social Security number, and/or vaccination status. Please note that we have no reason to believe that this information was viewed or downloaded by any person. Rather, we believe the information was only accessed by an automated bot agent. There is no evidence that any of the information has been or will be publicly disclosed, or that any information was or will be misused for fraudulent purposes as a result of this incident, but we are communicating this to you so that you can take the steps outlined below to protect yourself.

What We Are Doing

Upon initial detection of the unauthorized activity, we immediately took containment steps and commenced an investigation with the assistance of cybersecurity experts. We also reset your password so that the password that the unauthorized third parties obtained from some other source would no longer enable access to your Aya account.



0000399



M8894-L01

We understand this may feel unsettling and we want to make sure you feel secure. Therefore, we're offering you free access to Experian IdentityWorks credit monitoring and remediation services for 24 months. These services will notify you of any changes to your credit file for two years from the date of enrollment and offer support with any questions or fraud-related issues.

How do I enroll for the free services?

Identity restoration assistance is immediately available to you, and we also encourage you to activate the fraud detection and credit monitoring tools available through Experian IdentityWorks. To enroll in these services at no charge, visit www.experianidworks.com/credit 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 by May 30, 2025. 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.

Should you have any questions regarding the Credit Monitoring services, have difficulty enrolling, or require additional support, please contact Experian at 833-931-7577. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the Identity Restoration services by Experian.

What You Can Do

To help protect your personal information, we strongly recommend you take the following steps, all of which are good ideas in any event:

- Use a different password for each of your online accounts. If you use the same password for multiple sites, a security breach on one site could allow others to access your other accounts.
- Enroll in the free credit monitoring service that we are offering to you. This will enable you to get alerts about any efforts to use your name and social security number to establish credit and restoration assistance if you were not the one who initiated it.
- Carefully review statements sent to you by your bank, credit card company, or other financial institutions as well as government institutions like the Internal Revenue Service (IRS). Notify the sender of these statements immediately by phone and in writing if you detect any suspicious transactions or other activity you do not recognize.
- The attached **Reference Guide** describes additional steps that you can take and provides resources for additional information. We encourage you to read and follow these steps as well.

For More Information

If you have questions or concerns not answered by this letter, please contact Aya Healthcare at 866-687-7390. Please know that we take this matter very seriously, and we apologize for any concern this may cause.

Sincerely,



Amber Zeeb
Chief People Officer
and EVP of Global Services and Infrastructure

REFERENCE GUIDE

If you suspect that you are a victim of identity theft or credit fraud, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the FTC's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number. When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible if there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer credit reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumerfinance.gov> or www.ftc.gov.

Place a Fraud Alert on Your Credit File: A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below.

Equifax

www.equifax.com

1-800-525-6285

P.O. Box 740241

Atlanta, Georgia 30374-0241

Experian

www.experian.com

1-888-397-3742

P.O. Box 9532 Allen,

Texas 75013

TransUnion

www.transunion.com

1-800-680-7289

Fraud Victim Assistance Division

P.O. Box 2000

Chester, Pennsylvania 19016

Place a Security Freeze on Your Credit File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus using the same contact information noted above.

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide: (1) Your full name (including middle initial as well as Jr., Sr., II, III, etc.); (2) Social Security number; (3) Date of birth; (4) If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years; (5) Proof of current address, such as a current utility bill or telephone bill; (6) A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and (7) If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft.

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe your identity has been stolen, the FTC recommends that you take these additional steps.

0000399



- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

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

For District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 20001, 202-727-3400, www.oag.dc.gov.

For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, <https://www.marylandattorneygeneral.gov>.

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
<https://ag.ny.gov>

NYS Department of State's Division of
Consumer Protection
(800) 697-1220
<https://www.dos.ny.gov/consumerprotection>

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge but note that consumer reporting agencies may charge fees for other services.