# Morgan Lewis



**Gregory T. Parks**
Partner
215.963.5170
gregory.parks@morganlewis.com

**VIA FIRST CLASS MAIL**

January 24, 2020

State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

*Re:* *Notification of Potential Breach of Security*

Dear Office of the Attorney General:

This firm represents a number of Medicaid and Medicare health plans that are part of the AmeriHealth Caritas Family of Companies ("AmeriHealth Caritas"), including Select Health of South Carolina, Inc., AmeriHealth Caritas Health Plan, AmeriHealth Caritas Delaware, Inc. and Keystone Family Health Plan, in connection with an incident believed to have impacted some New Hampshire residents.

This incident arose when an AmeriHealth Caritas employee, who has since been terminated, refused to cooperate in ensuring the secure destruction of company information, including personal information of health care providers credentialed by the aforementioned AmeriHealth Caritas health plans, after the employee inappropriately downloaded this information to a personal hard drive installed on company-issued equipment, against company policy. Based upon its investigation, AmeriHealth Caritas has reason to believe that one of the files on the hard drive included the first and last names, dates of birth, and Social Security Numbers of 11 providers residing in New Hampshire. AmeriHealth Caritas promptly notified law enforcement, and is cooperating with their investigation and actively seeking confirmation whether they have acquired the hard drive and destroyed the provider data.

While AmeriHealth Caritas does not presently have reason to believe that the former employee intended to misuse or re-disclose this information, or any reason to believe that this information has been misused or re-disclosed, AmeriHealth Caritas is notifying you in an abundance of caution. AmeriHealth Caritas also plans to send notification letters to the affected providers by January 24, 2020, and offer them two-year subscriptions to Experian IdentityWorks' credit monitoring and identity theft protection services. Further information about what AmeriHealth Caritas has done and is recommending to the affected individuals can be found in the enclosed notification letter template.

If you have any questions, please feel free to contact me.

Regards,

Gregory T. Parks

Enclosures

**AmeriHealth Caritas**
200 Stevens Drive
Philadelphia, PA 19113

January 24, 2020

ACFC_Provider_168
***For Addressee Only***
[Provider name]
[Address 1]
[Address 2]
[City, State Zip]

**Re: Personal Information Potentially Compromised**

Dear [Provider name]:

We are writing to tell you about a data security incident that may have exposed some of your personal information. While we have no reason to believe that this information has been or will be used inappropriately, we would like to let you know what happened, what information was involved, what we have done to address the situation, and to remind you of what you can do to protect your continued privacy.

**What Happened?**

Through its affiliated companies, the AmeriHealth Caritas Family of Companies ("AmeriHealth Caritas") operates a network of health plans across a number of states.* On or about November 15, 2019, we learned that a former AmeriHealth Caritas employee improperly downloaded company confidential information to a personal hard drive. On that day, we contacted him and requested that he surrender the hard drive or co-operate with us to ensure that the contents of the hard drive had been erased, but he refused to do either. Based upon our investigation, we have reason to believe that the downloaded information included files containing personal information of a number of our providers, including you.

**What Information Was Involved?**

The files on the hard drive may have included personal information about you, including your first and last name and your social security number. To date, we have not received any reports of improper use of any of this information. Nor do we have any reason to believe that the former employee will use any of this information for any improper purposes.

**What We Are Doing?**

The security and privacy of your information is of utmost importance to us. Immediately upon learning of the former employee's refusal to co-operate, we took steps to determine what information was on the hard drive and to notify appropriate authorities. We contacted law enforcement promptly and are pursuing appropriate action through law enforcement concerning the former employee and the information on the hard drive. We also are looking into changes to our controls and procedures to reduce the risk of similar events occurring in the future.

What You Can Do

There are several steps you can take to protect your continued privacy and be sure that your information is not used improperly, many of which are good practices in any event.

First, in an abundance of caution, to help protect your identity, we are offering a complimentary two-year subscription to Experian's® credit monitoring and identity theft protection service, IdentityWorks. This product helps detect possible misuse of your personal information and provides you with superior identity theft detection and resolution support. To activate your membership and start monitoring your personal information please follow the steps below:

**Activate Experian IdentityWorks Now in Three Easy Steps**

1. **Ensure that you enroll by:** March 31, 2020 (Your code will not work after this date.)
2. **Visit the Experian IdentityWorks website to enroll:** https://www.experianidworks.com/credit
3. **Provide your activation code:** [ACTIVATION CODE]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-716-5553** by **March 31, 2020**. Be prepared to provide engagement number **DB16594** as proof of eligibility for the identity restoration services by Experian.

**Additional details regarding your 24-month Experian IdentityWorks membership:**

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **877-716-5553**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Second, contact any financial institutions that you bank with and advise them of this situation, particularly if any of them use your social security number to identify or verify you. Check your accounts online or via telephone for any potential fraudulent activity. You should check your periodic statements from each such financial institution or credit card company promptly upon receiving them to be sure that no unauthorized transactions have occurred, and remain vigilant for incidents of fraud and identity theft.

Third, you should review any explanations of benefits, account statements, transaction confirmations that you receive by mail or email or any other similar communications you receive from institutions that you know. If you find any activity you do not recognize or that seems suspicious, you should contact the sender of that information immediately.

**For More Information**

For general information on protecting your privacy and preventing unauthorized use of your personal information, you may visit the U.S. Federal Trade Commission's Web site, http://ftc.gov or contact your state office of consumer affairs or attorney general. You can also see the enclosed "Reference Guide" for more information relevant to your state.

* * *

We are committed to maintaining the security and privacy of the personal information you entrusted to us. We apologize for any inconvenience or concern this incident may cause. If we can be of any further assistance or answer any questions, please call **877-716-5553**.

Sincerely,

Tyrina D. Blomer, Esq.
Vice President, Corporate Compliance and Privacy Officer
AmeriHealth Caritas Family of Companies

***Health Plans Operating Within the AmeriHealth Caritas Family of Companies**

| | | |
|---|---|---|
| AmeriHealth Caritas Delaware | AmeriHealth Caritas District of Columbia | AmeriHealth Caritas Louisiana |
| AmeriHealth Caritas New Hampshire | AmeriHealth Caritas North Carolina | AmeriHealth Caritas Northeast |
| AmeriHealth Caritas Pennsylvania | AmeriHealth Caritas Pennsylvania Community HealthChoices | Blue Cross Complete of Michigan |
| First Choice VIP Care Plus® by Select Health of South Carolina | Keystone First | Keystone First Community HealthChoices |
| AmeriHealth Caritas VIP Care® | PerformCare® | Prestige Health Choice |
| First Choice by Select Health of South Carolina | Keystone First VIP Choice® | AmeriHealth Caritas VIP Care Plus® |

## REFERENCE GUIDE

In the event that you suspect that you are a victim of identity theft, 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 U.S. Federal Trade Commission'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 in the event 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 reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov

**Place a Fraud Alert on Your Credit File:** To protect yourself from possible identity theft, consider placing 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. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

| | | | |
|---|---|---|---|
| Equifax | P.O. Box 740241<br>Atlanta, Georgia 30374-0241 | 1-800-525-6285 | www.equifax.com |
| Experian | P.O. Box 9532<br>Allen, Texas 75013 | 1-888-397-3742 | www.experian.com |
| TransUnion | Fraud Victim Assistance Division<br>P.O. Box 2000<br>Chester, Pennsylvania 19016 | 1-800-680-7289 | www.transunion.com |

**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 at:

| | | |
|---|---|---|
| Equifax | P.O. Box 740241<br>Atlanta, Georgia 30374-0241 | www.equifax.com |
| Experian | P.O. Box 9554<br>Allen, Texas 75013 | www.experian.com |
| TransUnion | Fraud Victim Assistance Division<br>P.O. Box 2000<br>Chester, Pennsylvania 19016 | www.transunion.com |

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 the following information:

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.)
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.

**Report Incidents.** 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 you identity has been stolen, the FTC recommends that you take these additional steps.

- 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 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, www.oag.state.md.us

**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/internet/resource-center

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 obtain a police report and place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services.