

RECEIVED

Humana

July 25, 2023

JUL 31 2023

SP 01 000002 65691 H 1 ASNGLP

DEPT. OF CONSUMER
AFFAIRS



South Carolina Identity Theft Unit Re: S
Notification

South Carolina Department of Consumer Af
PO Box 5757
Columbia, SC 29250

RE: Case # 582893

NOTICE OF PRIVACY INCIDENT

Dear South Carolina Identity Theft Unit Re: Security Breach Notification- South Carolina Department of Consumer Affairs,

The purpose of this letter is to provide your office notice of a privacy incident that impacted residents of your state.

What Happened?

Humana has a contract with Purfoods, LLC DBA Mom's Meals, to provide meals and post-discharge and chronic care nutrition to Humana members.

On February 22, 2023, Mom's Meals experienced an incident involving suspicious account behavior that included the encryption of certain files within their network. They responded to the incident immediately and began an investigation with the assistance of outside cybersecurity specialists. Through their response efforts, they learned that an unauthorized actor obtained access to certain Mom's Meals systems between January 16, 2023, and February 22, 2023. During that period, some information stored on the Mom's Meals network was acquired by the unauthorized actor, and other information was accessible and potentially viewed. Upon containing the incident and reconnecting their computer systems, Mom's Meals began to review the potentially affected data to determine whether it contained any identifiable personal information. There were **17,660** residents of your state impacted.

What Information Was Involved?

The data involved in the Mom's Meals incident was voluminous and complex. The review confirmed that Humana member data was impacted. We have determined that due to the limited information that Humana shares with Mom's Meals, and the fact that some of our members maintain a direct relationship with Mom's Meals outside of their plan benefits, accurate reconciliation of data between Mom's Meals and Humana is not possible. Therefore, we are unable to identify the exact Humana plans of the impacted members. Nevertheless, both Mom's Meals and Humana recognize the importance of issuing notifications to all impacted individuals for awareness and to protect themselves. Because of these extenuating circumstances, Humana is only able to provide an understanding of impacted members by state of residence.

The type of information impacted in this incident varies by individual and could have included: name, address, date of birth, driver's license, Social Security number, banking information, medical record number, Medicare or Medicaid identification number, Mom's Meals identification number, provider name, and claims, diagnosis, and/or treatment information. Mom's Meals is scheduled to mail notifications to all impacted individuals beginning in early August.

What We Are Doing

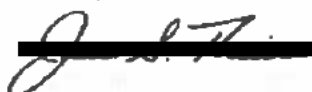
Humana takes this incident and the security of information entrusted to us very seriously. In response to the incident, Mom's Meals promptly took steps to mitigate any risk of compromise to information. They immediately notified the FBI of the event. Other actions included: (1) migrated all systems and applications to Azure; (2) contracted with third-party cybersecurity companies to perform internal and external penetration testing, monitor their network and remediate any suspicious activity identified; (3) rebuilt all network servers and storage; (4) enforced multi-factor authentication across their enterprise. Mom's Meals is also enhancing existing training protocols and other internal procedures that relate to data protection and security. Please note that there is no evidence or other indication that identity theft or fraud occurred as a result of this incident, but Mom's Meals is encouraging individuals to review account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately.

Mom's Meals is providing impacted individuals with access to free identity monitoring and restoration services through Kroll, along with guidance on how to protect against the possibility of information misuse.

Humana will promptly report to your office and appropriate law enforcement officials any information that is shared with us that indicates this information has been inappropriately used.

Please do not hesitate to contact me if you have any additional questions regarding this situation.

Sincerely,



James S. Theiss
Associate VP, Privacy & Ethics
Humana Inc.
502-580-4322
jtheiss@humana.com

Attachments

[PurFoods LLC Company Header/Logo]

<<Return Mail Address>>

<<Name 1>> <<Name 2>>

<<Address 1>>

<<Address 2>>

<<City>>, <<State>> <<Zip>>

<<Country>>

RECEIVED

JUL 31 2023

<<Date>>

DEPT. OF CONSUMER
AFFAIRS

Dear <<Name 1>>:

As part of our vital mission of improving life through better nutrition at home, PurFoods, LLC [doing business as Mom's Meals ("PurFoods")] may have provided you with one or more meal(s). We are writing to notify you of a recent event that may involve some of your personal information, as well as our response to the event and steps you can take to protect that information, should you feel it appropriate to do so.

What Happened? Upon identifying suspicious account behavior on February 22, 2023, we launched an investigation with the help of third-party specialists. The investigation determined that we experienced a cyberattack between January 16, 2023, and February 22, 2023, that included the encryption of certain files in our network. Because the investigation also identified the presence of tools that could be used for data exfiltration (the unauthorized transfer of data), we are not able to rule out the possibility that data was taken from one of our file servers.

What Information Was Involved? Third-party specialists have helped us conduct a review of the potentially involved data, which concluded on July 10, 2023, and determined that the files at issue included your name and [Extra 2 – Data Elements].

It's important to note that we have seen no evidence that any personal information was misused or further disclosed as a result of the cyberattack.

What We Are Doing. We have notified Federal law enforcement of this event and cooperated with their subsequent investigation. Further, because safeguarding the privacy of information in our care is one of our highest priorities, we have taken a number of steps to further strengthen our network security. We also are reviewing our existing policies and procedures to identify additional measures and safeguards.

What You Can Do. We encourage you to be watchful about potential identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity, as well as by reading the attached *Steps You Can Take to Protect Personal Information*. Though we are not aware of any actual or attempted misuse of your personal information, as an added precaution, we have arranged to offer you access to twelve (12) months of complimentary credit monitoring and identity restoration services provided through Kroll. We are unable to enroll you directly, but we have included enrollment instructions in the attached *Steps You Can Take to Protect Personal Information*.

For More Information. We are sorry for any inconvenience this incident may cause. If you have additional questions, please call us at [insert phone number], Monday through Friday, from X:00

a.m. to X:00 p.m. Central Time. You may also write to PurFoods, LLC at 3210 SE Corporate Woods Drive, Ankeny, IA 50021.

Sincerely,

Jane Sturtz
Privacy Officer

CONFIDENTIAL

RECEIVED

JUL 31 2023

DEPT. OF CONSUMER
AFFAIRS

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

To help relieve concerns and restore confidence following this incident, Purfoods has secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.

You have until **<<Date>>** to activate your identity monitoring services.

Membership Number: [REDACTED]

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

Examine Insurance Correspondence

Because the personal information in question may have included your health insurance member identification number, we encourage you to carefully review explanations of benefits (EOBs) and other correspondence from your insurer to ensure you actually received the services. If not, you can contact your insurance company's customer service line to report any discrepancies.

How to Monitor Your Accounts

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Freezes and Fraud Alerts

You also have the right to place a "credit freeze," at no cost to you, on your credit report, which will prohibit a credit bureau from releasing information in your credit report without your express authorization. This is designed to prevent credit, loans, and services from being approved in your name without your consent, and you can lift the freeze at any time. While credit is frozen, however, approvals for new loans, credit cards, mortgages, or other accounts involving the extension of credit could be delayed. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

As an alternative to a credit freeze, you also can place either an initial or extended "fraud alert" on your credit report, also at no cost. An initial fraud alert is a 1-year alert that is placed on a credit file. Upon seeing a fraud alert display, a business is required to take steps to verify your identity before extending new credit. If you are a victim of identity theft, you are entitled to a seven-year extended fraud alert lasting seven years.

To learn more about credit freezes and fraud alerts, please visit the Federal Trade Commission's website at <https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts>. Should you wish to place a credit freeze or either type of fraud alert, please contact any one of the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	1 (800) 916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You can find more information on protecting your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint by writing them at 600 Pennsylvania Avenue NW, Washington, DC 20580; visiting www.identitytheft.gov; or calling 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

In addition, you have the right to file a police report if you ever experience identity theft or fraud. When filing a report with law enforcement for identity theft, you will likely be asked to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. Please note, this notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

RECEIVED

JUL 31 2023

000002 4/4

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/ff/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.