VIA U.S. MAIL

September 14, 2023

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

RE: Notification of Aetna vendor PurFoods (Mom's Meals) Information Security Incident

Dear Attorney General Brown:

Aetna Life Insurance Company ("Aetna") is writing to notify the Office of the Maryland Attorney General (the "Attorney General") that a security incident that occurred at one of its vendors, PurFoods LLC dba Mom's Meals ("PurFoods") was determined to have affected 4 Maryland residents. PurFoods is a vendor used by Aetna to provide post-hospital discharge meal delivery services. Aetna is providing this notice to the Department in accordance with applicable Maryland law**.** Please note that no Aetna system or service, and no data maintained by Aetna, was involved in this data breach.

I. Brief Description of the Breach

On February 22, 2023, PurFoods discovered suspicious account activity on their network and launched an investigation with the support of a third-party cybersecurity firm. The investigation determined that PurFoods experienced a cyberattack between January 16, 2023, and February 22, 2023, that included the encryption of certain files within their network. The investigation also identified the use of tools that could be used for data exfiltration (the unauthorized transfer of data), and PurFoods was not able to rule out the possibility that data was taken from one of their file servers.

After a detailed analysis and review of the potentially involved data, which concluded on July 10, 2023, PurFoods determined that the files included personal and protected health information related to certain individuals. The information that could have been subject to unauthorized access include name, driver's license/state identification number, medication information, health information, and date of birth.

II. How PurFoods Responded

PurFoods retained a third-party forensics firm that handles cyber incidents and breach response, to assist in the investigation. The parties involved have no evidence that any personal information was used or further disclosed as a result of the cyberattack. PurFoods has notified Federal law enforcement of the cyberattack and cooperated with their subsequent investigation. In addition, PurFoods reported that they have taken several steps to further strengthen their network security and provide additional training to its employees. PurFoods is also evaluating

existing policies/procedures and implementing new tools and technologies to recognize and prevent potential threats to its data.

PurFoods provided written notice of the incident on August 25, 2023, to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

III. How Aetna Responded

PurFoods notified Aetna of this incident in February 2023. In February and March of 2023, PurFoods reported that they would be conducting a comprehensive review of any data to determine what type of data was possibly accessed and exfiltrated and who the data belonged to. On or about July 11, 2023, PurFoods provided notice that it could not rule out the possibility that data was taken from its servers. Aetna worked diligently and expended considerable time and resources to obtain and review the information. Aetna required additional information, including additional information on the members potentially impacted and the impacted data files to identify Aetna reporting obligations and member impact. On August 22, 2023, PurFoods provided Aetna with the necessary information.

In accordance with the obligations set forth at 45 C.F.R. §164.404 (notifications to individuals by a HIPAA covered entity) and Maryland law, PurFoods will be issuing notification on Aetna's behalf to the impacted members by first class U.S. mail as well as offering 12 months of complimentary identify and credit monitoring through Kroll. PurFoods began notifying affected individuals on behalf of Aetna on September 13, 2023. A draft of the notice that will be sent to the affected individuals is attached. PurFoods is also notifying other federal, and state regulatory agencies as required by law.

I want to assure you that Aetna expects its vendors to adhere to the highest of privacy standards. If you have any questions, you may contact me at 609-313-2608 and jeremy.abidiwan-lupo@cvshealth.com or by mail at CVS Health Privacy Office, One CVS Drive Woonsocket, RI 02859.

Sincerely,

Jeremy Abidiwan-Lupo
Privacy & Security Counsel

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>>:

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) as part of our relationship with Aetna. 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? On February 22, 2023, we noticed suspicious account behavior on our network and 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 us being locked out from 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 review the potentially involved data, which concluded on July 10, 2023, and determined that the files at issue included your <<b2b_text_1(name, data elements)>>. The incident did not involve your Social Security number or any financial or banking information.

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 Help 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 identity monitoring services provided through Kroll. We are unable to activate you directly, but we have included activation instructions in the attached *Steps You Can Take to Help 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 (866) 676-4045, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time (excluding major U.S. holidays). You may also write to PurFoods, LLC at 3210 SE Corporate Woods Drive, Ankeny, IA 50021.

Sincerely,

Jane Sturtz
Privacy Officer

STEPS YOU CAN TAKE TO HELP 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 **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

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 https://www.marylandattorneygeneral.gov/.

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/f/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 699 Rhode Island residents impacted by this incident.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

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