



December 15, 2023

VIA EMAIL

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

idtheft@oag.state.md.us

Re: Data Security Incident

Dear Office of the Attorney General:

Aetna is writing to notify the Maryland Attorney General's Office representative that it recently determined that a security incident that occurred at one of our vendors, PayFlex impacted one (1) Maryland resident who are/were a member of a fully insured Aetna medical plan. 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 November 16, 2023, PayFlex, notified us they became aware of suspicious activity on one (1) Maryland residents HSA. PayFlex immediately launched an investigation and took steps to lock and protect the account.

Personal information was obtained about this member from an unknown source and was used to access the member's PayFlex online account on November 6 and 7, 2023. PayFlex determined that personal information that may have been accessed includes the following types of information: full name, Social Security number (SSN), date of birth, mailing address, internal HSA number, username, email address, phone number, HSA tax forms, and healthcare provider claim data may have been viewed by the malicious actor. No funds were removed from the HSA.

II. How PayFlex Responded

In response to this incident, PayFlex is offering credit monitoring for two (2) years at no cost to the resident. To take advantage of this protection, the resident should follow the enclosed Experian instructions and activate coverage by the deadline stated in the enrollment information. PayFlex has also included general information on steps residents can take to guard against identity theft and fraud.

PayFlex will contact the resident to help them regain online access to their HSA.

III. How Aetna Responded

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, PayFlex will be issuing notification on Aetna's behalf to the impacted member by first class U.S. mail. The member breach mailing date has not yet been determined. A draft of the notice that will be sent to the affected individual is attached.

I want to assure you that Aetna expects its vendors to adhere to the highest of privacy standards. If you have any questions about this incident, please contact me.

Regards,

A handwritten signature in black ink, appearing to read "Shannon Wood". The signature is fluid and cursive, with a long horizontal stroke at the end.

Shannon Wood | Lead Director, Aetna Privacy Office
p 215-775-0316
1425 Union Meeting Road, Mail Code: U23S, Blue Bell, PA 19422

Notice of Breach of Security System
To the Maryland Insurance Commissioner

This Notice of Breach form must be completed if the carrier: (i) conducts an investigation required under § 14-3504(b) or (c) of the Commercial Law Article; and (ii) determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused.

Company Name: Aetna ACE

Name of person filing this Notice: Shannon Wood Phone Number: 215-775-0316

Email Address: woodse@aetna.com

Provide a brief description of the circumstances of the security breach.

See attached notification to the Attorney General.

In addition to the above, this Notice must be accompanied by the following documents:

- A form copy of all notifications sent to consumers as a result of the security breach.
- A copy of the notice of a breach of the security of a system submitted to the Maryland Attorney General, as required under § 14-3504(h).

MARYLAND INSURANCE ADMINISTRATION

MARKET CONDUCT ACTION

CERTIFICATE OF COMPLIANCE

Pursuant to Code of Maryland Regulations (“COMAR”) 31.04.20.05 E, I Shannon Wood hereby certify to the best of my knowledge, information, and belief, that the information hereto submitted to the Maryland Insurance Administration (“Administration”) represents a full, complete, and truthful Notice, as required under Insurance Article, § 4-406, Annotated Code of Maryland.

I further attest that I am an authorized officer/representative of the Company, that I have undertaken an adequate inquiry to provide this certification to the Commissioner, and am authorized to bind the company to the responses provided.

Signature: _____

Print Name: Shannon Wood

Company: Aetna ACE

Title: Lead Director, Privacy Office

Date: 12/15/2023



[Mail date TBD]

Your Experian Activation Code: insert code

Dear Member,

As you are aware, we have identified unauthorized access to your Health Savings Account (HSA) that is administered for Federal Employee Health Benefit Program by PayFlex. This letter describes how your account was impacted and the steps we are taking to protect your account.

Here is what happened

We identified suspicious activity related to your HSA on November 8, 2023. We immediately launched an investigation and took steps to protect your account. Personal information about you was obtained from an unknown source and was used to access your HSA online on November 6 and 7, 2023.

Types of information involved

Personal information on your PayFlex online HSA including your name, Social Security number (SSN), date of birth, mailing address, internal HSA bank number, username, email address, phone number, HSA tax forms, and health transaction data, including healthcare provider names, *may* have been viewed. No funds were removed from your account.

How PayFlex responded

We have temporarily disabled access to your account via the PayFlex site until we can contact you to coordinate setting up a new username and password for your online HSA.

Protection of your information

In response to this incident, we are offering credit monitoring for two (2) years at no cost to you. To take advantage of this protection, please follow the attached Experian instructions and activate your coverage no later than January 31, 2024. We are also including general information on more steps you can take to guard against identity theft and fraud.

Once you have regained access to your HSA online, we encourage you to review and confirm that all of your personal information (phone number, email address, bank account, beneficiaries, etc.) is accurate. We suggest that you

monitor your HSA as you would a bank account and immediately report any suspicious activity to PayFlex at 844-729-3539/844-PAYFLEX.

We sincerely regret any inconvenience or concern caused by this incident. If you have any questions about this incident, please feel free to call me directly at 630-422-6872, or you may request a call back from me via the toll-free customer service number, 844-729-3539/844-PAYFLEX.

Sincerely,

Clark Anderson
Director of Investigative Services
PayFlex Systems USA, Inc.
630-422-6872

What we are doing to protect your information:

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: January 31, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: SYR4Z4GG8**

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 877.890.9332 by **January 31, 2024**. Be prepared to provide engagement number **B108105** 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 877.890.9332. 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 24 months 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.

[This page left blank intentionally.]

How to Protect Your Identity

Protecting your Identity

Remember to look at your account statements regularly to be sure they are correct.

Ask for a free copy of your credit report:

- Online at www.annualcreditreport.com
- By calling toll-free 1-877-322-8228
- By mailing an Annual Credit Report Request Form (found at www.annualcreditreport.com) to:

Annual Credit Report Request Services
P. O. Box 105281 Atlanta,
GA 30348-5281

You can also buy a copy of your credit report from any of the companies listed below.

Experian P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
Equifax P.O. Box 740241, Atlanta, GA 30374-0241, 1-800-685-1111, www.equifax.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

What to look for in your reports

When you receive your credit reports, review them carefully.

Look for accounts or creditor inquiries that you did not make or do not recognize. Be sure information like home address and social security number is correct.

If you don't understand your credit report, call the number on the report.

Keep watching your credit reports and account statements.

If information doesn't look right or you suspect identity theft, you can contact:

- Any credit monitoring company you have enrolled with
- Your local police
- Your state's attorney general
- The Federal Trade Commission ("FTC")

You can also contact the FTC or your state's regulatory authority to get more information about avoiding identity theft.

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

For residents of Maryland: You can also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You can also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Protecting your Personal Health Information

- You should always review the explanation of benefits statement that you get from your health insurance company. If it shows services you did not receive, contact your insurance company at the number on the statement.
- If you don't get statements directly, contact your provider and ask for copies.
- Ask your provider for a copy of your medical records so you can compare them to your statements.
- You can also get a copy of your credit report and look for medical bills you don't recognize.
- If you don't understand your credit report, call the number on the report.
- Keep a copy of this notice in case you have problems with your medical records later on.

For residents of California: You can also visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov for more information about your medical privacy.

Fraud Alerts

Fraud alerts let your creditors know you may be a victim of fraud.

There are two types of fraud alerts that can be placed on your credit report. The two types of fraud alerts are an initial alert and an extended alert.

You can have an initial alert put on your credit report if you think you may be a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days.

You can have an extended alert put on your credit report if you know you are a victim of identity theft and can show proof. An extended fraud alert stays on your credit report for seven (7) years.

To put a fraud alert on your credit report, just call any one of the national credit reporting agencies below.

Experian:	1-888-397-3742	www.experian.com
Equifax:	1-888-766-0008	www.equifax.com
TransUnion:	1-800-680-7289	fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents)

You may have the right to put a credit freeze on your credit file. A credit freeze is also known as a security freeze.

A credit freeze will stop new credit from being opened in your name without a PIN number. The PIN number is given to you when you ask for the freeze.

A credit freeze also stops possible credit grantors from getting your credit report without your consent. You will need to lift the freeze every time you want to give a credit grantor or other third-party access to your credit report. This means that using a credit freeze may delay your credit approval.

You may be charged fees to place, lift, or remove a credit freeze.

The cost can vary by state from \$5 to \$20 for each service and each credit reporting company.

To place a credit freeze on your file you must contact each credit reporting company separately. The instructions for getting a credit freeze vary from state to state.

For more information about fraud alerts and credit freezes, you can contact the FTC or the credit agencies below:

Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
TransUnion:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com