ahp | Academic HealthPlans

21826

June 21, 2021

[redacted]

Dear [redacted]

Academic HealthPlans, Inc. ("AHP") is committed to protecting the confidentiality and security of the information we maintain. This letter constitutes notice of an incident that may have involved some of Aetna's information. To date, we do not have any evidence that indicates that student member information was actually accessed or misused, but we are notifying you of this incident out of an abundance of caution.

On May 3, 2021, we concluded our investigation of an email phishing incident that targeted AHP's employees. The investigation determined that two AHP employees' email accounts were subject to unauthorized access as a result of the incident between the dates of August 6, 2020 and August 24, 2020, and on October 2, 2020. Although we did not find any evidence that indicates that any emails or information were exported from the employees' email accounts or that any protected health information ("PHI") was targeted or actually viewed, we could not definitively rule out that possibility. The investigation confirmed that the unauthorized access was limited to AHP's cloud-based, Microsoft Office 365 email system and did not involve AHP's enrollment waiver platform or any other AHP systems.

Subsequently, in order to determine if any PHI contained in the emails related to your member students[1], we reviewed, both programmatically and manually, the information contained in the employees' email accounts. Based on this review, we determined that emails or attachments in the employees' email accounts contained at least one or more personal information data elements, including names, dates of birth, Social Security numbers, health insurance member numbers, claims information, and diagnoses, and treatment information. We have been working since then to identify which covered entities these individuals are affiliated with and identify what information was accessible by student.

Our investigation determined that this incident potentially involved the information of current and former student members. AHP is prepared to take the following actions on your behalf:

1. Notify current and former student members whose information may have been involved in this incident.. Copies of the proposed notification letters are attached.[2]

2. Provide current and former members whose Social Security numbers were verified to be contained in the employees' email accounts with complimentary memberships to credit monitoring services;

[1] In limited circumstances, information pertaining to spouses and/or dependents of member students may have been involved.

[2] Notice letters will be tailored to each individual and will be revised to comply with applicable state breach notification laws.

3. Notify applicable federal regulators, specifically, the United States Department of Health and Human Services' Office for Civil Rights, and any applicable state regulators, to the extent required by applicable law;

4. Post notice on our website of the incident and provide you with a URL link so that you can add a link to your website;

5. Issue a press release where required by HIPAA regulations; and

6. Establish a dedicated call center to respond to questions about this incident.

Please let us know by June 25, 2021, if you do NOT want AHP to provide these services.

AHP takes this incident very seriously and, as part of our ongoing efforts to help prevent something like this from happening in the future, we are re-educating our employees regarding phishing emails and enhancing existing security measures. We sincerely regret that this incident occurred and apologize for any concern it may cause you or your members.

If you have any questions, please email privacyofficer@ahpcare.com or call 1-833-212-7696.

Sincerely,

Brett Curran

Brett Curran
Compliance Director

Enclosure: Sample Individual Notice Letters

ahp | Academic HealthPlans

[Sample Notice Letter to Individuals whose SSNs were Involved]

<<Name 1>><<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>> <<Date>>

Dear <<Name 1>><<Name 2>>:

Academic HealthPlans, Inc. ("AHP") is the insurance broker for **<<University / College Name>>** and helps to administer your student health insurance plan. We are committed to protecting the security and confidentiality of all the information we maintain. We are writing to inform you about an incident involving some of your health plan information. This notice explains the incident, measures we have taken, and some steps you can take in response. To date, we do not have any evidence that indicates that your information was actually accessed or misused, but we are notifying you of this incident out of an abundance of caution.

On **[Date]**, we notified **<<Health Insurance Carrier Name>>** of an email phishing incident that targeted AHP employees and may have resulted in unauthorized access to emails and attachments in the employees' email accounts. The investigation determined that two AHP employees' email accounts were subject to unauthorized access as a result of the incident between the dates of August 6, 2020 and August 24, 2020, and on October 2, 2020. Although we did not find any evidence that indicates that any emails or attachments were exported from the employees' email accounts or that any information was targeted or actually viewed, we could not definitively rule out that possibility. The investigation confirmed that the unauthorized access was limited to AHP's cloud-based, Microsoft Office 365 email system and did not involve AHP's enrollment waiver platform or any other AHP systems.

Subsequently, in order to determine if any emails or attachments contained personal information, we reviewed, both programmatically and manually, the information contained in the employees' email accounts. Based on this review, we determined that emails or attachments in the employees' email accounts contained information about you, including your name in combination with your **<<Type of PHI involved for Individual>>**

We recommend that you regularly review the explanation of benefits received from your health insurer. If you see services that you did not receive, please contact the insurer immediately. As a precaution, we have secured the services of Experian® to offer you a complimentary one-year membership of Experian's IdentityWorks℠. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks is completely free and enrolling in this program will not hurt your credit score. **For more information on IdentityWorks, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take to protect your information, please see the pages that follow this letter.**

We regret any inconvenience or concern this may cause you. To help prevent a similar incident from occurring in the future, we have provided extensive training to our employees regarding phishing emails and other cybersecurity issues, and have enhanced existing security measures. If you have any questions, please call **<<XXX-XXX-XXXX>>**, Monday through Friday, **<<X:XX a.m. to X:XX p.m.>>**, Central Time.

Sincerely,

Brett Curran

Brett Curran
Compliance Director

4841-5808-4568.13
4841-5808-4568.15

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **EXPIRATION DATE** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: URL
3. PROVIDE the **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 **PHONE NUMBER**. Be prepared to provide engagement number **ENGAGEMENT NUMBER** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

A. **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
A. **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
B. **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
C. **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at URL
or call PHONE NUMBER to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at **PHONE NUMBER**.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. Please refer to the actual policies for terms, conditions, and exclusions of coverage.

ahp | Academic HealthPlans

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit. *How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. *How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Connecticut Residents: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

District of Columbia Residents: You may contact and obtain information from your attorney general at: *Office of the Attorney General for the District of Columbia*, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Maryland Residents: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

Massachusetts Residents: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Office of the Massachusetts Attorney General,* One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

New York Residents: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina Residents: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island Residents: Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia Residents: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.

- Identity theft victims and active duty military personnel have additional rights.

ahp | Academic HealthPlans

[Sample Notice Letter to Individuals whose SSNs were NOT Involved]

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name 1>>:

Academic HealthPlans, Inc. ("AHP") is the insurance broker for **<<University / College Name>>** and helps to administer your student health insurance plan. We are committed to protecting the security and confidentiality of all the information we maintain. We are writing to inform you about an incident involving some of your health plan information. This notice explains the incident, measures we have taken, and some steps you can take in response. To date, we do not have any evidence that indicates that your information was actually accessed or misused, but we are notifying you of this incident out of an abundance of caution.

On **[Date]**, we notified **<<Health Insurance Carrier Name>>** of an email phishing incident that targeted AHP employees and may have resulted in unauthorized access to emails and attachments in the employees' email accounts. The investigation determined that two AHP employees' email accounts were subject to unauthorized access as a result of the incident between the dates of August 6, 2020 and August 24, 2020, and on October 2, 2020. Although we did not find any evidence that indicates that any emails or attachments were exported from the employees' email accounts or that any information was targeted or actually viewed, we could not definitively rule out that possibility. The investigation confirmed that the unauthorized access was limited to AHP's cloud-based, Microsoft Office 365 email system and did not involve AHP's enrollment waiver platform or any other AHP systems.

Subsequently, in order to determine if any emails or attachments contained personal information, we reviewed, both programmatically and manually, the information contained in the employees' email accounts. Based on this review, we determined that emails or attachments in the employees' email accounts contained information about you, including your name in combination with your **<<Type of PHI involved for Individual>>**

We recommend that you regularly review the explanation of benefits received from your health insurer. If you see services that you did not receive, please contact the insurer immediately.

We regret any inconvenience or concern this may cause you. To help prevent a similar incident from occurring in the future, we have provided extensive training to our employees regarding phishing emails and other cybersecurity issues, and have enhanced existing security measures. If you have any questions, please call **<<XXX-XXX-XXXX>>**, Monday through Friday, **<<X:XX a.m. to X:XX p.m.>>**, Central Time.

Sincerely,

Brett Curran

Brett Curran
Compliance Director