

Notice of Data Incident

Pennsylvania Adult & Teen Challenge (“PAATC”) is notifying individuals of an event that may affect the privacy of some personal information. While, to date, we have no evidence that information has been or will be misused, we are providing information about the event, our response to it, and resources available to help protect personal information.

What Happened? On or about July 29, 2020, we noticed suspicious activity involving an employee email account. In response, we immediately took steps to investigate this activity, change all user accounts passwords, and disable the compromised account. From this investigation, we determined that an unauthorized person(s) gained access to certain employee email accounts between July 27, 2020 and July 30, 2020. The forensic investigation could not conclusively determine whether or what information in the accounts may have been accessed. Based on this, in an abundance of caution, we undertook a detailed and diligent review of all data present in the accounts to determine what records were present at the time of the incident, to whom those records related, and the contact information for those individuals. This comprehensive review process was completed on or around December 29, 2020.

While, to date, the investigation has found no evidence of actual or attempted misuse of data, we are making our community aware in an abundance of caution.

What Information Was Involved? PAATC’s investigation learned that certain information related to PAATC patients was within the impacted accounts. While the information varies by individual, it may include Social Security Number, driver’s license number, financial account information, payment card information, date of birth, prescription information, diagnosis information, treatment information, treatment provider, health insurance information, medical information, Medicare/Medicaid ID number, employer identification number, electronic signature, username and password.

What Is PAATC Doing? PAATC takes the confidentiality, privacy and security of the personal information in our care seriously. Upon learning of unusual activity in an employee email account, we immediately commenced an investigation to confirm the nature and scope of the event and identify what personal information may have been present in the affected emails accounts. With the assistance of third-party forensic investigators, we have been working to identify and put in place resources to assist potentially affected individuals and are implementing additional safeguards to further protect the security of information in our systems. We will also be reporting this incident to the U.S. Department of Health and Human Services and state regulators, as appropriate.

What Can Individuals Do? Please review the information listed below in the “Steps You Can Take to Protect Personal Information” section of this page.

For More Information. We recognize that individuals may have questions that were not addressed. If you have additional questions, please contact our dedicated assistance line at 888-905-0063, Monday – Friday, 9am to 9pm Eastern.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Identity Monitoring

If you were affected by this incident, your mailed notice letter will include enrollment information and instructions.

Monitor Accounts

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

You have the 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should

be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

PO Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

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 a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need 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. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General can be contacted at 441 4th St. NW #1100 Washington, D.C. 20001; by phone at 202-727-3400; and by email at oag@dc.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

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