Adult & Teen Challenge
Pennsylvania

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: Notice of Data Incident

Dear <<Name 1>>:

Pennsylvania Adult and Teen Challenge ("PAATC") writes to notify you of an incident that may affect the privacy of some of your personal information. While, to date, we have no evidence that your information has been misused, we are making you aware of the event, our response, and steps you may take to better protect your information, should you feel it appropriate to do so.

What Happened? On July 29, 2020, PAATC became aware of unusual activity related to an employee's email account. PAATC immediately took steps to investigate this activity, change all user account passwords, and disable the relevant account. PAATC also began working with forensic specialists to investigate the nature and scope of the incident. From this investigation, PAATC 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, PAATC 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, PAATC is notifying individuals whose information was potentially accessible within the accounts.

What Information Was Involved? Our investigation determined that the following information related to you was present in the email accounts at the time of the incident: name and <<data elements>>.

What We Are 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.

As an added precaution, we are offering you access to <<12/24>> months of credit monitoring and identity theft restoration service at no cost to you. The cost of these services will be paid for by PAATC. More information on these services, as well as instructions about how to enroll, may be found in the enclosed "Steps You Can Take to Protect Personal Information." Please note that you must complete the enrollment process, as we are not able to enroll you in these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity and to detect errors. You may also find more information in the enclosed "Steps You Can Take to Protect Personal Information," as well as details on how to enroll to receive the credit monitoring and identity restoration services we are offering at no cost to you.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 888-905-0063 (toll free), 9am- 9pm Eastern Time.

We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Heather Powell

Heather Powell
Vice President, Human Resources and Compliance
Pennsylvania Adult & Teen Challenge

Steps You Can Take to Protect Personal Information

Enroll in Identity Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<12/24>> months provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Account>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Engagement Number>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>.** Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR <<12/24>> -MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain <<12/24>> months of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

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 listed below 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	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	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/.