



Eckert Seamans Cherin & Mellott, LLC
U.S. Steel Tower
600 Grant Street, 44th Floor
Pittsburgh, PA 15219

TEL: 412 566 6000
FAX: 412 566 6099

Matthew H. Meade, Esq.
(412) 566-6983
mmeade@eckertseamans.com

March 24, 2023

Via Email: IDTheft@oag.state.md.us

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

Re: Notice of Data Security Incident

Dear Attorney General Brown:

This notice is provided on behalf of my client, Adams County Children and Youth Services (“ACCYS”), following an incident that involved the names, dates of birth, health information and/or Social Security numbers of twenty-four (24) Maryland residents. ACCYS is a department of Adams County, Pennsylvania (the “County”). ACCYS will provide written notice to impacted individuals later today, via U.S. Mail. The notice letter includes general advice on how to protect one’s identity and obtain free credit reports and security freezes, as well as instructions for enrolling in a one-year, complimentary membership with Experian for credit monitoring and identity theft services for those whose unredacted Social Security number was potentially impacted. A copy of a sample notice letter is enclosed and additional details on the incident are below.

On August 15, 2022, an ACCYS employee responded to a phishing email. The County immediately changed that employee’s password. Recently, as part of the County’s ongoing evaluation of email security and with the assistance of a nationally recognized digital forensics team, the County discovered that there had been suspicious activity on the same employee’s email box that the County was not aware of at the time of the password change. The County worked with the investigators to further understand what happened. Through the investigation the County learned that an unauthorized individual accessed the email account for approximately 30 minutes. ACCYS could not determine which specific emails were accessed. In an abundance of caution, ACCYS decided to review the entire contents of the email box to establish what information may have been involved, who may have been affected, and where those people reside so that it could provide notice.

Because of this incident, the County has taken steps to ensure the security of all email accounts and worked to review the contents of the impacted email account. To further strengthen the security of the information the County maintains, and to help prevent similar incidents in the future, it has taken or will be taking the following steps:

1. Completed implementation of multi-factor authentication on ACCYS employee email accounts;
2. Enhancing the retention policy for electronic data;

3. Retraining ACCYS employees regarding protection of private information in email communications;
4. Supplementing training for employees regarding cybersecurity awareness; and
5. Implementing automatic password reset procedures for cybersecurity incidents.

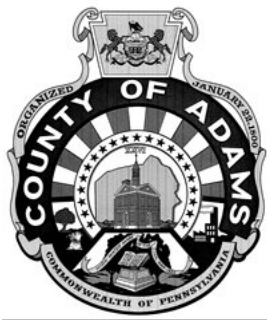
Additionally, ACCYS will provide notice of this incident to the United States Department of Health and Human Services and appropriate state regulators.

Please do not hesitate to contact me if you have any questions or concerns.

Sincerely,

/s/ Matthew H. Meade, Esq.

MHM/
Enclosure



Adams County Children and Youth Services

ADMINISTRATOR

SARAH A. FINKEY

ASSISTANT ADMINISTRATOR

SHERRI DEPASQUA, MSW, LSW

March 24, 2023



NOTICE OF DATA SECURITY INCIDENT

Dear [REDACTED]

We are writing to you to tell you about a recent incident at Adams County Children and Youth Services (ACCYS) that may have involved your personal information. We take this matter very seriously because we know how important your information is to you. **At this time, we are not aware of any misuse of your information.** Nonetheless, we are providing this notice to you as a precautionary measure, to inform you, offer complimentary identity monitoring services, and explain steps you can take to protect your information.

What Happened

On August 15, 2022, one of our employees responded to a phishing email. We immediately changed the employee's password. Recently, as part of our ongoing evaluation of email security and with the assistance of a nationally recognized digital forensics team, we discovered that there had been suspicious activity on the same employee's email box that we were not aware of at the time of the password change. We worked with the investigators to further understand what happened and to determine the scope of any potential unauthorized access to the email box. We determined through the investigation that we would be unable to identify which specific emails may have been viewed or acquired by the unauthorized actor during the approximately 30-minute period of access. Therefore, in an abundance of caution, we undertook a comprehensive review of the entire contents of the email box to establish what information may have been involved, who may have been affected, and where those people reside so that we could provide notice.

What Information Was Involved

The impacted email account contained your name or initials, your Social Security number, as well as some or all of the following kinds of information: address, date of birth, names of family and/or household members, ACCYS case number(s) and/or referral number(s), information about residency and/or placements, personal family referral information, or information regarding services and programming provided by ACCYS.

What We Are Doing About It

Because of this incident we have taken steps to ensure the security of all email accounts and worked to review the contents of the impacted email account. To further strengthen the security of the information

HUMAN SERVICES BUILDING
525 BOYDS SCHOOL RD, SUITE 100 – GETTYSBURG, PA 17325
PHONE (717) 337-0110 - FAX (717) 337-0616

we maintain, and to help prevent similar incidents in the future, we have taken or will be taking the following steps:

1. Completed implementation of multi-factor authentication on ACCYS employee email accounts;
2. Enhancing our retention policy for electronic data;
3. Retraining ACCYS employees regarding protection of private information in email communications;
4. Supplementing our training for employees regarding cybersecurity awareness; and
5. Implementing automatic password reset procedures for cybersecurity incidents.

Additionally, we will provide notice of this incident to the United States Department of Health and Human Services and appropriate state regulators.

What You Can Do

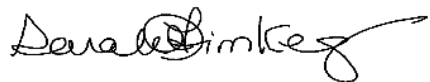
We recommend that you take the following preventative measures to help protect your information:

1. Enroll in a complimentary, one-year membership with Experian. This membership will provide you with identity monitoring services, including a copy of your credit report at signup; credit monitoring; identity restoration; Experian IdentityWorks ExtendCARE; and up to \$1 million in identity theft insurance. Instructions on how to activate your membership are included at the end of this letter.
2. Remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements, and free credit reports for any unauthorized or suspicious activity. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, can be found at the end of this letter.
3. Report any incidents of suspected identity theft to your local law enforcement, state Attorney General and the major credit bureaus.

For More Information

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and will continue to take many precautions to safeguard it. If you have any questions or concerns about this incident, you may contact us toll-free at (833) 475-1813, Monday through Friday 9 AM – 11 PM EST, Saturday and Sunday 11 AM – 8 PM EST (excluding major U.S. holidays). Please be prepared to provide the following engagement number: [REDACTED] You may also contact Adams County Privacy Officer, Lindsey Ringquist, at (717) 337-9820.

Sincerely,



Sarah A. Finkey
Administrator
Adams County Children and Youth Services

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit <https://www.experian.com/blogs/ask-experian/category/fraud-and-identity-theft/> for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.consumer.ftc.gov/features/feature-0014-identity-theft. The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

Equifax P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com	Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com
--	---	--

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at <https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0093-annual-report-request-form.pdf> and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report. You may be able to obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

Fraud Alerts

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. As soon as one credit bureau confirms the fraud alert, they will notify the others. Additional information is available at www.annualcreditreport.com.

Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone

line, or a written request to all three of the credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

After receiving your freeze request, each credit reporting company will send you a confirmation letter containing 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. If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

Additional Helpful Information

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them at the information provided above. This notice was not delayed as a result of a law enforcement investigation.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

STATE SPECIFIC INFORMATION

MARYLAND residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

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

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

TO ACTIVATE YOUR MEMBERSHIP AND START MONITORING YOUR PERSONAL INFORMATION PLEASE FOLLOW THE STEPS BELOW:

- Ensure that you **enroll by: 6/30/2023** (Your code will not work after this date).
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code:** [REDACTED]

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 **6/30/2023**. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian. 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, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** 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 as a result of this incident 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 from the date of the incident (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 12 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.

* 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.