



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

February 24, 2022

VIA EMAIL

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Frosh:

This notice is provided on behalf of my client, Fulton County, Pennsylvania (the “County”) following a data breach that involved the name, date of birth, address, Social Security number, and health information of sixteen (16) Maryland residents. The County will provide written notice to the affected 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 if an individual’s Social Security or driver’s license number was involved. A copy of the notice letter is enclosed and additional information about the incident is below.

In November of 2021, County employees began receiving reports of a high volume of spam emails. These emails often contained copies of internal County communications. As soon as the County learned about this, the County immediately engaged legal counsel and launched an investigation. Legal counsel also hired cybersecurity experts to assist with the investigation to better understand what happened, and, more importantly, help prevent something like this from happening again.

After an extensive investigation, the County learned that there had been incidents of data being removed from County email accounts between November 3, 2021 and November 7, 2021. Since then, the County worked with cybersecurity experts to review the contents of each affected email box in order to find out what information was in each email, who may have been affected and where those people reside so that it could provide proper notice. On January 21, 2022, the County learned that the data included the personal information of Maryland residents.

Because cyber threats are always evolving, the County continuously works to identify and mitigate threats when they occur and to evaluate its IT security protocols so that sensitive data is protected to the greatest extent possible. In addition, to further enhance email and network security

and to help prevent similar occurrences in the future, the County has taken or will be taking the following steps:

1. Transitioned its email to Microsoft 365 to improve overall security;
2. Adding two factor authentication for remote access;
3. Strengthening its filtering to help block dangerous emails;
4. Enhancing its cyber training and patch management procedures; and
5. Upgrading its servers.

In addition, consistent with its compliance obligations and responsibilities, the County is providing notice of this incident to appropriate federal and state regulators.

The County is committed to protecting the personal information in its possession and will continue to take steps to safeguard it. Should you have any questions or concerns, please do not hesitate to contact me.

Sincerely,

/s/ Matthew H. Meade, Esq.

MHM/
Enclosure



Fulton County Commissioners

116 West Market Street, Suite 203, McConnellsburg, PA 17233

Telephone: (717) 485-3691 Fax: (717) 485-9411 Email: commissioners@co.fulton.pa.us

Stuart L. Ulsh, Chair
Randy H. Bunch, Vice-Chair
Paula J. Shives

Lisa Mellott-McConahy, Chief Clerk
Jim Stein, County Solicitor

February 24, 2022

«First» «MI» «Last»
«Address»
«City», «State» «Zip»

NOTICE OF DATA SECURITY INCIDENT

Dear «First» «Last»:

We are writing to tell you about a recent incident that may have exposed personal information in the email boxes of employees of Fulton County (the "County") to unauthorized access. As a result of our investigation, we determined that some personal information that we maintained about a small number of individuals may have been accessed without authorization. We take this matter very seriously because we know how important your personal information is to you. We are providing this notice to you as a precautionary measure, to inform you and to explain steps that you can take to protect your information.

What Happened

In November of 2021, County employees began receiving reports of a high volume of spam emails. These emails often contained copies of internal County communications. As soon as we learned about this, we launched an investigation to understand what happened and, more importantly, to prevent something like this from happening again. As a result of the investigation, we learned that there had been incidents of data being removed from County email accounts between November 3, 2021 and November 7, 2021.

What Information Was Involved

Because we could not identify what specific information was accessed we reviewed the contents of each affected email box in order to find out what information was in each email, who may have been affected and where those people reside so that we could provide proper notice. Based upon our investigation, that information may have included your name, address, date of birth, driver's license number or Social Security number, the fact that you were receiving services from CYS, and other medical information, such as health history, medication and treatment information, test results, health insurance number, provider name, dates of service, and demographic information about family members. The specific information is dependent on the County department or office that you dealt with or that provided services to you.

What We Are Doing About It

When we discovered this incident, we scanned our email system to detect unauthorized activity. To further enhance email and network security and to help prevent similar occurrences in the future, we have taken or will be taking the following steps:

1. Transitioned our email to Microsoft 365 to improve our overall security;
2. Adding two factor authentication for remote access;
3. Strengthening our filtering to help block dangerous emails;
4. Enhancing our cyber training and patch management procedures; and
5. Upgrading our servers.

In addition, consistent with our compliance obligations and responsibilities, we are providing notice of this incident to appropriate federal and state regulators.

What You Can Do

Although we are not aware of any inappropriate use of your personal information, we are notifying you so that you can take steps to protect yourself. We recommend that you remain vigilant to the possibility of fraud and identify theft by reviewing and monitoring your account statements and free credit reports for any unauthorized activity. If you find any unauthorized or suspicious activity, you should contact local law enforcement.

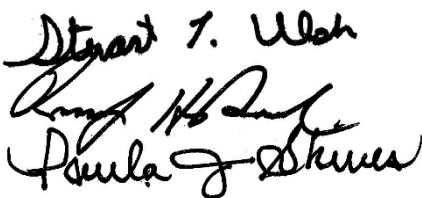
We strongly encourage you to take the following preventative measures to help detect and mitigate any misuse of your information:

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, free credit reports and health insurance Explanation of Benefits (EOB) forms 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 by calling us at 800-752-2806 between the hours of 8:00 a.m. and 4:30 p.m. EST, Monday through Thursday.

Very truly yours,



Stuart T. Ulan
Amy H. [unclear]
Paula J. [unclear]

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit www.experian.com/credit-advice/topic-fraud-and-identity-theft.html 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 1-888-909-8872 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 www.consumer.ftc.gov/articles/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.

For Maryland and New Jersey residents: You may 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 at least 90 days. 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.

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: May 31, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code: «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 **877.890.9332** by **May 31, 2022**. Be prepared to provide engagement number **B027981** 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 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 one year 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.