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

Fulton County
Notice of Data Breach

Fulton County (the "County") recently discovered that there may have been unauthorized access to some County emails. On February 24, 2022, the County sent letters to the last known address of every individual whose personal information we believe was affected by this incident. Unfortunately, we did not have sufficient contact information to provide written notice to a small number of individuals.

Please call us, toll-free, at 800-752-2806 between 8:00 a.m. – 4:30 p.m. Monday through Thursday to determine whether your information was involved in the breach. This number will be active through May 25, 2022. ***A copy of the letter that would have been provided to these individuals is provided below***:

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, the following types of information about your or your relative may have been involved: name, address, date of birth, driver's license number or Social Security number, payment card number with or without the accompanying CVV code and expiration date, the fact that you or your relative 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 or your relative dealt with or that provided services to you or your relative.

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 the personal information involved in the incident, we are notifying you so that you can take steps to protect this information. 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 this information:

1. Call the County to determine if your driver's license or Social Security number was involved. If it was, then you should 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.

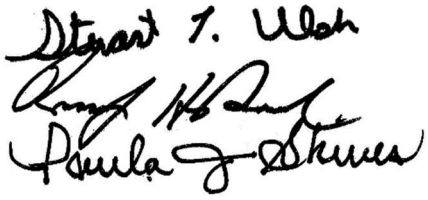
2. Remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements, free credit reports and health insurance Explanation of Benefits (EOB) forms for any unauthorized or suspicious activity. Information on additional ways to protect your information, including 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,



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	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	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.

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.