



BUTLER COUNTY NOTICE OF DATA SECURITY INCIDENT

Recently, Butler County (the “County”) determined there had been unauthorized access and acquisition to one email account related to the County jail. We take this matter very seriously because we are committed to the privacy and security of all information in our possession. **At this time, we are not aware of any misuse of the information involved in this incident.** Nonetheless, we are providing this notice to inform potentially impacted individuals and suggest ways that individuals can protect their information.

What Happened

On August 8, 2023, we learned that one County employee’s email account was sending unauthorized spam emails. Upon discovering this, we immediately worked to secure the employee email account. Thereafter, we conducted an investigation with the assistance of a nationally recognized digital forensics team, to further understand what happened and whether there was unauthorized access to the email box. On August 23, 2023, we determined there was unauthorized access to the County employee’s email account for a limited period of time on August 8, 2023, and that the contents of the email box appeared to have been copied by the unauthorized actor. Once we learned this, we began a thorough review of the 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. Although that review is ongoing, on August 31, 2023 we determined that personally identifiable information was impacted by this incident. Therefore, as required under Pennsylvania law, we are providing this notification while we continue the review of the contents of the email box. Upon completing our review, we will provide written notice to individuals and will offer complimentary credit monitoring services where appropriate.

What Information Was Involved

Our review of contents of the email account is ongoing; however, we have determined the emails may contain the following types of information: Social Security numbers, driver’s license numbers and/or medical information related to jail operations.

What We Are Doing About It

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

1. Securing impacted email account by changing password;
2. Retrained employee regarding cybersecurity practices related to email;
3. Communicated with all staff regarding increased awareness of phishing emails;
4. Enhancing internal policies and procedures related to cybersecurity;
5. Evaluating email retention policy; and
6. Ongoing investigation of additional tools, training, and third-party monitoring partnerships to strengthen security.

What You Can Do

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

1. Remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements, free credit reports, and any health insurance Explanation of Benefits (EOB) forms for 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.
2. 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 at (724) 431-1940, Monday through Friday, 8:30 AM to 4:30 PM.

Sincerely,

A handwritten signature in black ink, appearing to read 'James Venturini', with a stylized flourish at the end.

James Venturini
Director of Information Technology

September 12, 2023

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 <https://consumer.ftc.gov/features/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.

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.