February 9, 2023

Tattnall County, Georgia
Notice of Data Security Incident

To Whom It May Concern,

On December 14, 2022, Tattnall County (the "County") learned that some data had been removed from one County hard drive without authorization during a recent ransomware attack. On February 9, 2023, we mailed notifications to individuals whose protected health information and/or personally identifying information may have been subject to unauthorized access or acquisition. Unfortunately, we did not have sufficient contact information to provide written notice to some individuals. To notify those individuals for whom we do not have sufficient contact information, we are posting this notice on our website and providing a toll-free telephone number, **(833) 848-3403,** which can be called between 8 AM and 5 PM EST, Monday through Friday to determine whether an individual's personal information was included in the data impacted by this incident.

At this time, we have no indication that any of this data has been inappropriately used by anyone. However, we are providing this notice on our Tattnall County website as a precautionary measure, to inform potentially impacted individuals, and suggest ways that individuals can protect their information. We recommend that you closely review the information provided below for some steps that you may take to protect yourself against potential misuse of your information.

What Happened

On December 11, 2022, we detected a ransomware attack on our computer network. We immediately reported this to law enforcement and hired a nationally recognized digital forensics firm to understand what happened, contain the attack, and determine the scope of the incident. On December 14, 2022, we learned that some data had been removed from one County hard drive without authorization during the ransomware attack. Through the investigation, we determined that we would be unable to identify what specific information was accessed or removed from the affected hard drive. In an abundance of caution, we immediately began an extensive review of the data in the hard drive to determine 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 affected data varied, but may have included an individual's name, address, date of birth, checking account and routing number associated with an account used to pay for services provide by Tattnall County Emergency Medical Services ("County EMS"), medical codes associated with transportation by County EMS, date(s) an individual received services from County EMS, patient identification number and/or patient account number related to County EMS, information related to an individual's health insurance plan, and billing and payment information related to County EMS. For a small number of impacted individuals, the information may have included their Social Security number, driver's license number, other government identification number, and/or information related to their medical condition, diagnosis, injury, medications, or treatment, and/or the name of the hospital where they were transferred by County EMS.

What We Are Doing About It

When we discovered this incident, we immediately worked to secure our network and begin an investigation. Our investigators also searched Dark Web sources and found no indication that any of our data had been released or offered for sale as a result of this incident. To further enhance our security and to help prevent similar occurrences in the future, we have taken or will be taking the following steps:

1. Increasing antivirus protection,
2. Strengthening firewall capabilities,
3. Enhancing multi-factor authentication, and
4. Transitioning secure cloud-based storage for County data.

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

What You Can Do

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

1. Remain alert for incidents of fraud and identity theft by regularly reviewing any account statements, free credit reports and 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.

3. If an individual's Social Security number or driver's license number was involved, the County is offering credit monitoring services at no cost to the affected individual.

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.

Sincerely,

Jackie C. Trim
Chairman
Tattnall County Board of Commissioners

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	**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 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 this notice letter states that your financial account number and/or credit or debit card number was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account(s), including whether you should close your account(s) or obtain a new account number(s).

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.