Important Update from Wichita County, Texas

Wichita County wishes to inform the public about a recent cybersecurity incident. Following the detection of this incident, we have undertaken an immediate and thorough investigation. It has been determined that there was unauthorized access to our network, which has resulted in the potential exposure of legally protected personally identifying information. We are undergoing a comprehensive, manual review of all affected data to determine the individuals whose information may have been involved. Once that review is completed, affected individuals with available address information will be notified of the incident via U.S. First-Class Mail. Please know that we are working diligently to have the information reviewed as quickly as possible.

We are taking decisive steps to address this issue:

- We have engaged leading cybersecurity experts to assist with our investigation and to bolster our network security.
- Measures are being put in place to enhance our systems' resilience against future cyber threats.
- We are in the process of performing a comprehensive review of the impacted data to identify the affected individuals and effectuate formal notification via U.S. First-Class Mail. All individuals notified of the incident will be provided with information and resources to assist them with protecting their information.

While we are working as quickly as possible, the process of reviewing the impacted data is expected to take some time, so we wish to remind all community members to exercise diligence to monitor their credit reports, bank statements, and other sensitive documents closely and promptly report any suspicious activity to their financial institution. While we continue to review the affected data, we are providing the following specific information to the general public regarding steps that individuals can take to protect their information:

How can I find out if I was one of the individuals whose information was involved?

All individuals determined to have had information affected will receive a formal notification letter via U.S. First-Class Mail upon completion of the review process. We understand that it may be frustrating to not have all the information yet, but we are working diligently to have all information reviewed to identify these individuals and get notifications out as quickly as possible.

What steps can I take to protect my information?

- If you detect suspicious activity on any of your accounts, you should promptly notify the financial institution or company with which the account is maintained. You should also report any fraudulent activity or any suspected incidents of identity theft to law enforcement.
- You may obtain a copy of your credit report at no cost from each of the three nationwide credit reporting agencies. To do so, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. Contact information for the three agencies appears below.
- Notify your financial institution immediately of any unauthorized transactions made, or new accounts opened, in your name.

- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.

What should I do to protect myself from payment card/credit card fraud?

We suggest that you review your debit and credit card statements carefully in order to identify any unusual activity. If you see anything that you do not understand or that looks suspicious, you should contact the issuer of the debit or credit card immediately.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. To do so, please visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. Contact information for the three agencies is provided below.

How do I put a fraud alert on my account?

You may consider placing a fraud alert on your credit report. This fraud alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact Equifax, Experian or TransUnion and follow the Fraud Victims instructions. To place a fraud alert on your credit accounts, contact your financial institution or credit provider. Contact information for the three nationwide credit reporting agencies is listed below.

Contact information for the three nationwide credit reporting agencies is as follows:

Equifax Security Freeze	Experian Security Freeze	TransUnion (FVAD)
PO Box 105788	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

How do I put a security freeze on my credit reports?

Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. In order to place a security freeze, you may be required to provide the consumer

reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from the Texas Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Texas Attorney General:

Federal Trade Commission	**Texas Attorney General**
600 Pennsylvania Ave, NW	PO Box 12548
Washington, DC 20580	Austin, TX 78711
consumer.ftc.gov, and	texasattorneygeneral.gov
www.ftc.gov/idtheft	1-800-621-0508
1-877-438-4338	

We apologize for any inconvenience this may cause and appreciate your understanding and support as we work diligently to resolve this matter.