NOTICE OF CYBER INCIDENT

September 24, 2025

Union County (the "County") is notifying individuals about a ransomware attack that involved unauthorized access to and acquisition of protected personal information held by the County. We take this matter very seriously because of our commitment to the privacy and security of all County information. Beginning on September 24, 2024, we mailed notifications to individuals whose personal information was impacted by this incident. Unfortunately, we did not have sufficient contact information to provide notice to some individuals. We are posting this notice on our website and providing a toll-free telephone number to notify those individuals for whom we do not have sufficient contact information. The toll-free number can be found below.

What Happened

On May 18, 2025, the County detected ransomware on our computer network. As soon as we learned this, we immediately launched an investigation with assistance from nationally recognized third-party cybersecurity and data forensics consultants to secure our network and investigate the scope of the incident. We also alerted federal law enforcement. Through our investigation, we determined that the cyber criminals accessed our network from May 6, 2025 through May 18, 2025 and took some County data. We then conducted a thorough review of the impacted data to determine: (1) what information was involved; and (2) who may have been affected. On August 25, 2025, we completed that review and began locating mailing addresses for individuals whose information was impacted in order to provide written notice of this incident.

What Information Was Involved

We have determined that the affected personal information includes: name, Social Security number, driver's license/state identification card number, financial account information, date of birth, fingerprint information, medical information, payment card information, and passport number.

What We Are Doing About It

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. Deployed security tools to enhance detection and accelerate response to cyber incidents;
2. Continuing to actively monitor its network using end point detection tools;
3. Conducted enterprise-wide password reset;
4. Strengthened restrictions for external network access; and
5. Evaluating steps to further bolster our cyber defenses.

We also are monitoring internet sources and have found no indication that any personal information that we maintain has been released or offered for sale as a result of this incident. Additionally, the County will notify all appropriate state regulators regarding this incident.

What You Can Do

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

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

1. 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. The privacy and security of information is important to us, and we remain committed to protecting it. If you have any questions or concerns about this incident, you may call our dedicated assistance line at 1-833-919-4739, between 9:00 am and 9:00 pm Eastern time, Monday through Friday. Please be prepared to provide the following engagement number: B152377.

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	**Experian**	**TransUnion**
P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com	P.O. Box 2000 Chester, PA 19016 1-833-799-5355 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.