COUNTY OF LYCOMING

Return Mail Processing
PO Box 999
Suwanee, GA 30024

10 1 1779 **********AUTO**5-DIGIT 17701
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

December 9, 2025

NOTICE OF DATA SECURITY [Extra2]

Dear Sample A. Sample:

Lycoming County, Pennsylvania (the "County"), is writing to tell you about a ransomware attack that impacted data held by the County Department of Public Safety. We take this matter very seriously because of our commitment to the privacy and security of all County information. We are providing this notice to tell you about the incident, offer complimentary identity monitoring services, and suggest ways that you can protect your information.

What Happened

On August 12, 2025, the County detected ransomware on our computer network. 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 between August 11, 2025 and August 12, 2025 and took data. Once we learned this, we conducted a thorough review of the impacted data to determine: (1) what information was involved; (2) who may have been affected; and (3) where those individuals reside. On November 17, 2025, we completed our review and determined that your information was impacted by this incident.

What Information Was Involved

The impacted data included your [Extra1].

What We Are Doing About It

As soon as we learned about this incident, we immediately worked with our team to secure our network and begin an investigation. On August 27, 2025, we posted notice of this incident on the County website and notified major statewide media as required by Pennsylvania law. We have notified the Lycoming County District Attorney and will cooperate with any law enforcement investigation. We 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. 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. Enhanced capabilities of existing security tools to strengthen detection and accelerate response to cyber incidents;
2. Endpoint detection and response tools are running on endpoints;
3. Conducting enterprise-wide password reset; and
4. Strengthening restrictions for external network access.

Additionally, we are notifying all appropriate state regulators.

What You Can Do

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

1. Enroll in a complimentary, [Extra3]-month 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.

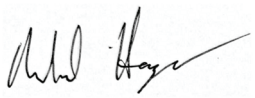
2. Remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and free credit reports for any unauthorized or suspicious activity. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, 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

The privacy and security of your information is very important to the County, and we remain committed to protecting it. If you have any questions or concerns about this incident, please call our dedicated assistance line at 833-918-5697 between 9:00 am to 9:00 pm Eastern time, Monday through Friday, excluding major holidays. Please be prepared to provide engagement number **[Engagement Number].**

Sincerely,



Michael Hagen
Chief Clerk

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	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-888-298-0045	1-888-397-3742	1-833-799-5355
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. 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. 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.

STATE SPECIFIC INFORMATION

DISTRICT OF COLUMBIA residents: You may also obtain information about preventing and avoiding identity theft from the D.C. Attorney General's Office. This office can be reached at:

Office of the Attorney General of the District of Columbia
Office of Consumer Protection
400 6th Street NW
Washington, D.C. 20001
www.oag.dc.gov
1-202-727-3400

MARYLAND residents: Lycoming County is located at 33 W 3rd St, 3rd Floor, Williamsport, PA 17701. You may also obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
https://www.marylandattorneygeneral.gov/
Toll-free: 1-888-743-0023

NEW YORK residents: You may also obtain information on identity theft from the New York Department of State Division of Consumer Protection or the New York Attorney General. These agencies can be reached at:

New York Department of State
Division of Consumer Protection
1-800-697-1220
http://www.dos.ny.gov/consumerprotection

New York Attorney General
1-800-771-7755
https://ag.ny.gov/

NORTH CAROLINA residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (Toll-free within North Carolina)
919-716-6000
www.ncdoj.gov

RHODE ISLAND residents: 2 Rhode Island resident(s) are impacted by this incident. You have the right to file and obtain a copy of a police report concerning any fraud or identity theft committed using your personal information. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General's Office. This office can be reached at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
Toll-free: 1-401-274-4400

ADDITIONAL DETAILS REGARDING YOUR [Extra3]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

TO ACTIVATE YOUR MEMBERSHIP AND START MONITORING YOUR PERSONAL INFORMATION PLEASE FOLLOW THE STEPS BELOW:

- Ensure that you **enroll by**: **March 31, 2026 (**Your code will not work after this date).
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **833-918-5697** by **March 31, 2026.** Be prepared to provide engagement number **[Engagement Number]** as proof of eligibility for the identity restoration services by Experian. A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **833-918-5697.** If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for [Extra3] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.