NOTICE OF DATA SECURITY INCIDENT
September 17, 2026

The Housing & Redevelopment Authority of Clay County (the "HRA") is notifying individuals about a recent ransomware attack that impacted protected information maintained by the HRA or Moorhead Public Housing Agency. We take this matter very seriously because we are committed to the privacy and security of all information in our possession. On September 17, 2026, we began mailing notification letters to impacted individuals.

We are providing this notice on the HRA website to inform potentially impacted individuals for whom we do not have sufficient contact information. If you have any questions regarding the incident, please call our dedicated call center at 1-888-202-2693, between 8:00 am and 8:00 pm Central Time, Monday-Friday, excluding major holidays. We have contracted this service provider to make sure that you receive the most accurate information possible regarding this matter. Please make sure to call this number directly. The person you work with at the HRA is not an expert in this area so will not be able to provide you with the best information available.

What Happened

On June 22, 2026, the HRA detected and responded to 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 determine the scope of the incident. We also notified federal law enforcement. Through the investigation, we learned that there was unauthorized access to the HRA network between June 19, 2026, and June 21, 2026. During that time, the cybercriminal copied some data from our network. Upon determining this, we began a thorough review of that data to determine: (1) what information was involved; (2) who may have been affected; and (3) where those people reside. On August 18, 2026, we completed that review and began working to provide written notice of this incident.

What Information Was Involved

The affected data included name, date of birth, Social Security number, driver's license number or state identification card number, passport number, immigration identification number, birth certificate, tribal identification card number, financial account number, health insurance identification number, medical or health information, and/or information related to services you or your family may have received from the HRA.

What We Are Doing About It

To further strengthen the security of the HRA's network and to help prevent similar incidents 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. Strengthening password policies across all users.
3. Actively monitoring our network using end point detection tools to help ensure containment.

4. Removed duplicative personal data from our internal system.
5. Enhancing protection of personal data maintained by the HRA; and
6. Conducting an enterprise-wide password reset.

Additionally, the HRA notified Minnesota IT Services and will notify all appropriate state regulators.

What You Can Do

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

1. Remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and free credit reports. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, can be found in the enclosed attachment.

2. Report any incidents of suspected identity theft to your local law enforcement, state Attorney General, and the major credit bureaus.

For More Information

We understand that this may be very upsetting for you. Please accept our apologies that this incident occurred. The privacy and security of your information is extremely important to us, and we remain committed to protecting it. To the best of our abilities, we are taking all steps available to reduce the impact that it may have on the affected population. The impacted individuals have the right to receive a report on the facts and details of the investigation into this incident. To request a copy of the report, please contact 1-888-202-2693, between 8:00 am and 8:00 pm Central Time, Monday-Friday, excluding major holidays. You may request delivery of the report via mail.

Once again, if you have any questions or concerns about this incident, please call this number for our contracted service professionals. The person you work with at the HRA is not an expert in this area so will not be able to provide you with the best information available. If you call the HRA offices, you will be re-directed to the above telephone number to make sure that you are receiving the most appropriate assistance.

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 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 <u>all three</u> 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.

<u>Protecting Your Medical Information</u>

We have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

<u>Additional Helpful Information</u>

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.