January 26, 2024

NOTICE OF DATA SECURITY INCIDENT

To Whom it May Concern.

Clay County, Minnesota ("Clay County") recently discovered a cyber incident that involved personal information related to individuals we serve and/or their household members. We take this matter very seriously because we are committed to the privacy and security of all information regarding the recipients of our services as well as the data that we host for other Minnesota Counties. **At this time, we are not aware of any misuse of any information involved in this incident**. On December 22, 2023, and January 26, 2024, Clay County mailed notifications to individuals whose protected health information and/or personal information was impacted by this incident. Unfortunately, we did not have sufficient contact information to provide written notice to some individuals. We are posting this notice on our website and providing a toll-free telephone number, (800) 459-5922, which can be called Monday through Friday, 8 AM to 8 PM CST (excluding major U.S. holidays), to notify those individuals for whom we do not have sufficient contact information. Please be prepared to provide the following Engagement Number: B114604.

What Happened

On October 27, 2023, Clay County determined that its network had been impacted by a ransomware attack that affected the electronic document management system ("CaseWorks"), which is hosted by Clay County and used by other Minnesota County social services entities. Clay County immediately initiated its incident response process and began working with its local information technology partner to investigate, to securely restore operations, and determine the effects of the incident. Clay County also worked with a nationally recognized digital forensics firm to assist with the investigation and notified federal law enforcement and the Minnesota Department of Human Services. Through the investigation, Clay County determined that there was unauthorized access to its network between October 23, 2023 and October 26, 2023. As Clay County continued its investigation, it later learned that cyber criminals responsible for this attack took some data from Clay County's network. As soon as Clay County learned this, it started notifying the other impacted counties and began an extensive review to determine what information may have been involved and who may have been affected, so that we could provide notice. Clay County recently completed that review and is providing notice to the identified impacted individuals.

What Information Was Involved

Based upon our investigation the affected data included an individual's name, together with some or all of the following kinds of information: Social Security number, address, date of birth, information regarding services provided to you by Clay County Social Services, such as locations of service, dates of service, client identification number or unique identifiers related to services provided to you, insurance identification number, and/or insurance or billing information.

What We Are Doing About It

Clay County's investigators searched Dark Web sources and found no indication that any personal information that the County maintains had been released or offered for sale as a result of this incident. To further enhance its security and to help prevent similar occurrences in the future, Clay County has taken or will be taking the following steps:

1. Implemented multi-factor authentication for any remote access to the CaseWorks application;
2. Updated procedures related to external access by any vendors;
3. Deployed security tools to enhance detection and accelerate response to cyber incidents; and

4.   Enhancing technical security related to the CaseWorks application.

In addition, consistent with the applicable compliance obligations and responsibilities, Clay County is providing notice of this incident to the United States Department of Health and Human Services and all appropriate state 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.

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. You have the right to receive a report on the facts and details of the investigation into this incident. If you would like a copy of the report, please contact the toll-free number to request delivery of the report via mail or email.

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 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-888-298-0045	1-888-397-3742	1-800-916-8800
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 <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.

<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.