Notice Regarding Data Incident

On December 6, 2024, two Iron County employees reported receiving a suspicious email from a third Iron County employee, directing the payment of an invoice. The two recipients immediately reported the emails as potentially suspicious. Iron County's personnel immediately reset all active sessions for all email accounts in its email tenant, launched its incident response plan, and engaged counsel. Iron County also engaged, through counsel, a reputable third-party forensics firm to assist with counsel's investigation.

The investigation concluded that the unknown threat actor was able to gain unauthorized access to a single email account. The evidence suggests that the unauthorized access was used to send two emails to Iron County employees, which were promptly detected and reported. There is no evidence any information related to the incident was otherwise actually misused and there was no evidence that emails were taken from the system, but we wanted to notify individuals out of an abundance of caution.

What Information Was Involved

The information involved differs from person to person. The investigation determined that potentially impacted data may have included an affected individuals' name, date of birth, date of service, doctor or provider name, employee ID, medical billing information, payment for health services information, incidental health reference, medical record number, procedure information, medical history, medical treatment information and other health insurance information.

What Iron County is Doing

Iron County took immediate steps to block the unauthorized access and to investigate the incident with the support of leading outside cybersecurity experts. Iron County deployed additional security measures and tools with the guidance of third-party experts to strengthen the ongoing security of its network.

Iron County is offering one year of complimentary identity protection services, which were included in the letters to the impacted individuals.

Letters to impacted individuals were mailed on June 30, 2025, including information regarding the complimentary identify protection services.

For a small number of individuals, we were not able to locate mailing addresses. *If you are concerned you may have been impacted, but have not received a letter, Iron County has set up a toll free number: 877-841-2712, Monday – Friday, 9 am – 9 pm Eastern Time, excluding U.S. holidays.*

Please be prepared to provide your full name, contact information, and your association with Iron County.

We encourage impacted individuals to take actions to help protect their personal information. These actions include enrolling in the credit monitoring services described, placing a fraud alert and/or security freeze on their credit files, and/or obtaining a free credit report. Additionally, individuals should always remain vigilant in reviewing their financial account statements, explanation of benefits statements and credit reports for fraudulent or irregular activity on a regular basis and report any suspicious activity to the proper authorities.

OTHER IMPORTANT INFORMATION

1. Placing a Fraud Alert.

We recommend that you place a one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax P.O. Box 105069 Atlanta, GA 30348-5069 www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (888) 378-4329; (800) 525-6285	***Experian*** P.O. Box 9554 Allen, TX 75013 www.experian.com/fraud/ center.html (888) 397-3742	***TransUnion*** Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016 www.transunion.com/fraud-alerts (800) 916-8800; 800-680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348-5788 www.equifax.com/personal/credit-report-services/credit-freeze/ (888) 298-0045; (800) 685-1111	***Experian Security Freeze*** P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze/ center.html (888) 397-3742	***TransUnion Security Freeze*** P.O. Box 160 Woodlyn, PA 19094 www.transunion.com/credit-freeze (800) 916-8800; (888) 909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information such as copy of a government issued identification. 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 a credit monitoring service, 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.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Protecting Your Medical Information.

If this notice letter indicates that your medical information was impacted, 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.

5. Additional Helpful Resources.

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 on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.