



# Dawson County

700 North Washington St Rm A, Lexington, NE 68850

Bill Stewart, Chairman  
PJ Jacobson, Vice-Chairman  
Dennis Rickertsen  
Rod Reynolds  
Richard Zarek

---

January 14, 2022

## **Dawson County Notice of Data Breach**

On September 25, 2021, Dawson County suffered a ransomware attack that impacted certain servers and workstations. Dawson County provided prompt notice to individuals whose protected health information we determined could have been accessed without authorization as a result of this attack. Unfortunately, we did not have sufficient contact information to provide written notice to a small number of these individuals.

**With regard to those individuals for whom we did not have sufficient contact information, we are providing a toll-free number below that can be called to determine whether an individual's health information was involved in the breach.**

*A copy of the letter that would have been provided to these individuals, had we had sufficient contact information, is provided below:*

The privacy and security of your personal information is of the utmost importance to Dawson County (the "County"). We are writing with important information regarding a recent data security incident that involved information that we store in connection with ongoing County operations, including information related to you. We wanted to tell you about the incident, suggest ways that you can help protect your information, and let you know that we continue to take significant measures to keep your information secure.

### **What Happened**

On September 25, 2021, the County suffered a ransomware attack that impacted certain servers and workstations. Once this happened, the County immediately started working with legal counsel

with expertise in cybersecurity. Legal counsel also hired nationally-recognized cyber security experts to assist with the investigation.

The County worked closely with its experts to understand what happened, contain the attack, and determine whether the incident involved personal information. The investigation revealed that the cybercriminals had accessed our computer network and removed some County data before deploying the ransomware. In order to convince us to pay the ransom, the cybercriminal provided us with a limited amount of County data in October. The County refused to pay the ransom. For this reason, the cybercriminal posted County data on the Dark Web on October 19, 2021. We immediately began an extensive review of this data to determine what information may have been involved, who may have been affected, and where those people reside so that we could provide notice. On November 22, 2021, we learned that the data included your personal information.

### **What Information Was Involved**

Based on our investigation, the impacted data included your name, date of birth, address, and certain health information used to administer claims, such as member identification number, provider name, and treatment information.

### **What We Are Doing**

We are committed to making this right and are investing in internal processes, tools, and resources to reduce the likelihood that this could happen again. Because cyber threats are always evolving, we are continuously working to identify and mitigate threats and evaluate our IT security protocols to make sure that sensitive data is protected. In addition, to further improve our network security and help prevent similar occurrences in the future, we have taken, or will be taking, the following steps:

- Deploying Sentinel One end point monitoring;
- Adding Multi-Factor Authentication;
- Strengthening backups and ability to recover data from backups;
- Closely monitoring and restricting outside access to our computer network;
- Increasing password complexity requirements;
- Strengthening our email filtering to help block dangerous emails;
- Updating our incident response procedures to more quickly and effectively respond to incidents; and
- Enhancing our cyber training and providing regular communications in order to increase cyber awareness.

In addition, consistent with our compliance obligations and responsibilities, we are providing notice of this incident to the Nebraska Attorney General and other appropriate state and federal regulators.

### **What You Can Do**

In an abundance of caution, we recommend that you take the following preventative measures to help detect and mitigate any potential misuse of your personal information:

1. Remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements, free credit reports and health insurance Explanation of Benefits (EOB) forms 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.
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.

**If you have any further questions regarding this incident, please contact us, toll-free, at (877) 565-8854, Monday through Friday, 8 a.m. to 10 p.m., CST, and Saturday and Sunday, 10 a.m. to 7 p.m. CST. Please be prepared to provide Engagement Number B023526 upon calling.**

Sincerely,

A handwritten signature in black ink that reads "Bill Stewart". The signature is written in a cursive, slightly slanted style.

Bill Stewart, Chairman  
Dawson County Board of Commissioners

## MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit [www.experian.com/credit-advice/topic-fraud-and-identity-theft.html](http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html) 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 [www.consumer.ftc.gov/features/feature-0014-identity-theft](http://www.consumer.ftc.gov/features/feature-0014-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

<b>Equifax</b> P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian</b> P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion</b> P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 <a href="http://www.transunion.com">www.transunion.com</a>
--	---	--

### 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](http://www.AnnualCreditReport.com) or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at [www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf](http://www.consumer.ftc.gov/articles/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.

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 at least 90 days. 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](http://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.

If this notice letter states that your financial account number and/or credit or debit card number was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account(s), including whether you should close your account(s) or obtain a new account number(s).

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.