



March 19, 2026

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear

The privacy and security of the personal information we maintain is of the utmost importance to Ernie's Store. We are writing to provide you with information regarding a recent cybersecurity incident that potentially involved your personal information. Please read this notice carefully, as it provides information about the incident, the complimentary identity monitoring services we are making available to you, and precautionary measures you can take to protect your information.

What Happened?

On or about June 19, 2025, we detected unauthorized access to our network.

What We Are Doing.

Upon learning of the issue, we secured our network and commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Following the completion of our investigation, it was determined that some of our files may have been accessed or removed by the unauthorized individual(s) on or about June 19, 2025. We conducted a thorough review of the potentially impacted data and on February 23, 2026, we determined that the impacted files may have contained your personal information.

What Information Was Involved?

The potentially impacted information includes

What You Can Do.

To date, we do not have evidence that your information has been used to commit financial fraud or identity theft. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and provide complimentary credit monitoring services as a precaution. We have secured the services of Kroll to provide identity monitoring at no cost to you for months. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. This letter provides more information about the complimentary services, enrollment instructions, and other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

If you have questions, please contact our dedicated and confidential call center at [REDACTED]. The response line is available between the hours of 8:00 a.m. to 5:30 p.m. Central Time, Monday through Friday, excluding major U.S. holidays. We have taken this matter very seriously and apologize for any inconvenience or concern this may cause. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

Sincerely,

Ernie's Store

318 South 2nd Street, Ceresco, NE 68017



1. Enrolling in Complimentary Credit Monitoring.

Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

- Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.
- You have until [REDACTED] to activate your identity monitoring services.
- Membership Number: [REDACTED]

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

Single Bureau Credit Monitoring: You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you’ll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Fraud Consultation: You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration: If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

2. 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

Equifax Information Services LLC
P.O. Box 105069,
Atlanta, GA 30348-5069
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
1-888-EQUIFAX (1-888-378-4329)

Experian

P.O. Box 9532,
Allen, TX 75013
www.experian.com/fraud
1-888-EXPERIAN (1-888-397-3742)

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000,
Chester, PA 19016
www.transunion.com/fraud-alerts
800-916-8800; 800-680-7289

3. 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

Equifax Information Services LLC
P.O. Box 105788,
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-888-EQUIFAX (1-888-378-4329)

Experian Security Freeze

P.O. Box 9554,
Allen, TX 75013
www.experian.com/freeze
1-888-EXPERIAN (1-888-397-3742)

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.

4. 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.

5. Protecting Medical Information.

As a general matter, the following practices can help deter, detect, and protect from medical identity theft. For more information visit consumer.ftc.gov/articles/what-know-about-medical-identity-theft. Only share health insurance cards with health care providers and other family members who are covered under the insurance plan or who help with medical care. Review the “explanation of benefits statement” which is provided by the health insurance company. Follow up with the insurance company or care provider for any items not recognized. 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 the insurance company for a current year-to-date report of all services paid for the impacted individual as a beneficiary. Follow up with the insurance company or the care provider for any items not recognized.

6. 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.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General’s Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.