

Koch Enterprises, Inc.  
c/o Cyberscout  
PO Box 179  
Manchester, NH 03105



July 26, 2024

**Re: Notice of Data** <<CUSTOM\_FIELD\_1>>

Dear <<FIRST\_NAME>> <<LAST\_NAME>>:

We are writing to inform you of a data security incident that may have affected your personal and/or protected health information. At South Western Communications, Inc. ("SWC"), we take the privacy and security of your information very seriously. That is why we are notifying you of the incident, providing you with steps you can take to help protect your information, and offering you complimentary identity protection services.

**What Happened.** On December 22, 2023, SWC experienced an encryption event that resulted in a network disruption. Upon discovering the incident, we swiftly took steps to secure our digital environment. We also engaged a digital forensics and incident response firm to conduct an investigation to determine whether any data may have been affected.

The investigation revealed that certain data stored on the SWC network may have been accessed or acquired without authorization between December 21, 2023, and December 22, 2023. SWC then undertook a comprehensive review of the potentially affected data. On July 10, 2024, we determined that some of your personal and/or protected health information was contained in the affected data. Since then, we have been working to gather contact information necessary to provide you with this notice.

**What Information Was Involved.** The potentially affected information may have included your name and <<EXPOSED\_DATA\_ELEMENTS>>

**What We Are Doing.** As soon as SWC discovered the incident, we took the steps described above and reported this incident to the Federal Bureau of Investigation. We also implemented additional measures to enhance the security of our digital environment and minimize the risk of a similar incident occurring in the future. As a further precaution, we are offering you complimentary identity protection services through Cyberscout, a TransUnion company. These services provide you with alerts for <<SERVICE\_LENGTH>> from the date of enrollment when changes occur to your credit file and include proactive fraud assistance to help with any questions you may have.

**What You Can Do.** We encourage you to review the recommendations included with this letter to help protect your information. In addition, you can enroll in the complimentary identity protection services by logging on to <https://bfs.cyberscout.com/activate> and following the instructions provided. When prompted please provide the following unique code to receive services: <<UNIQUE\_CODE>>. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. When prompted, please provide the unique code noted above to enroll in the services. For more information on how you can protect your personal information, please review the resources provided on the following pages.

0000102G0500

P

**For More Information.** If you have questions or need assistance, please call 1-833-531-2204, Monday through Friday from 7 a.m. to 7 p.m. Central, excluding holidays.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

South Western Communications, Inc.  
4871 Rosebud Lane  
Newburgh, IN 47630

## STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

**Copy of Credit Report:** You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

**Equifax**  
P.O. Box 105851  
Atlanta, GA 30348  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

**Experian**  
P.O. Box 9532  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016  
1-800-916-8800  
[www.transunion.com](http://www.transunion.com)

**Fraud Alert:** 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 one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

**Security Freeze:** You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

**Federal Trade Commission**  
600 Pennsylvania Ave, NW  
Washington, DC 20580  
[consumer.ftc.gov](http://consumer.ftc.gov), and  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
1-877-438-4338

**Maryland Attorney General**  
200 St. Paul Place  
Baltimore, MD 21202  
[oag.state.md.us](http://oag.state.md.us)  
1-888-743-0023

**New York Attorney General**  
Bureau of Internet and Technology  
Resources  
28 Liberty Street  
New York, NY 10005  
1-212-416-8433

**North Carolina Attorney General**  
9001 Mail Service Center  
Raleigh, NC 27699  
[ncdoj.gov](http://ncdoj.gov)  
1-877-566-7226

**Rhode Island Attorney General**  
150 South Main Street  
Providence, RI 02903  
<http://www.riag.ri.gov>  
1-401-274-4400

**Washington D.C. Attorney General**  
441 4th Street, NW  
Washington, DC 20001  
[oag.dc.gov](http://oag.dc.gov)  
1-202-727-3400

**You also have certain rights under the Fair Credit Reporting Act (FCRA):** These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.



