EBA/SSI LETTERHEAD/LOGO

INDIVIDUAL NAME
STREET ADDRESS
CITY, STATE AND POSTAL CODE

[DATE]

NOTICE OF DATA BREACH

Dear [INDIVIDUAL NAME]:

EB Archbald & Associates, Inc. provides energy production accounting services to oil and gas producers and operators. The process of providing our services necessitates the exchange of information between our office and our energy producer clients and includes, among other things, the names, postal information, and social security or federal tax identification numbers for individuals who hold an interest oil and gas wells.

We recognize and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your personal information. It is important to note that we have no evidence at this time that your information has been utilized for any fraudulent purpose as a result of this incident. However, we are sending this letter to tell you what happened, what information was potentially involved, what we have done and what you can do to address this situation. Please read this letter carefully as is provides you with what happened and what you can do about it.

WHAT HAPPENED?

On March 23, 2025, we discovered that our company had been the target of a so-called "ransomware" attack. The attackers hacked into our system and utilized software to encrypt all data on our servers and Microsoft cloud-based portal. In a subsequent communication the attackers demanded payment of a large sum of money in exchange for their release of a "decryption key". We immediately contacted the local office of the Federal Bureau of Investigation and notified them of the attack. Per recommendations received from the FBI we refused to meet the attackers' extortion demands. Five (5) days after their initial attack, and following our refusal to meet their monetary demand, we received a communication from the attackers claiming that they had downloaded information from our systems which they intended to release on the world wide web. Although the attackers have never provided any evidence to establish this claim, we cannot rule out the possibility that they accomplished an exfiltration of information and that they could follow through on their threat to release information.

WHAT INFORMATION WAS INVOLVED?

The data accessed potentially included your first name and last name, postal address social security number or federal tax identification number and bank account and routing information. We do not obtain or retain any account passwords, access codes driving license or other state issued identification numbers. As such, this information was not among the information potentially taken.

WHAT WE ARE DOING

Immediately upon discovering this incident EB Archbald & Associates, Inc. launched an investigation with the assistance of cybersecurity experts, law enforcement and outside lawyers. Determining whether any personal information was compromised in any way is one of our top priorities so that we can notify potentially affected individuals.

Be assured that we continue our work with outside cybersecurity experts to reinforce our systems and security protocols in an effort to prevent incidents like this one from occurring in the future including but not limited to upgrades to our web server infrastructure to improve date security; utilization of multi-factor authentication; and utilization of the very latest in cybersecurity software.

WHAT YOU CAN DO

We have partnered with IDX to answer questions and provide valuable information about the incident. We encourage you to contact IDX with any questions by calling [TFN]. IDX representatives are available Monday through Friday from 9:00 am to 9:00 pm Eastern Time.

Again, at this time there is no evidence that your information has been misused. IDX representatives have been fully apprised of the incident and can answer questions or concerns you may have regarding protection of your personal information.

MORE INFORMATION

You will find detailed instructions for enrollment in the enclosed Recommended Steps document.

Sincerely,

E. Baird Archbald
President

Recommended Steps to Help Protect Your Information

1. **Telephone.** Contact IDX at [TFN] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

2. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

3. Report suspicious activity. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

5. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

6. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** https://www.marylandattorneygeneral.gov, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-426