



SSI LETTERHEAD/LOGO

INDIVIDUAL NAME  
STREET ADDRESS  
CITY, STATE AND POSTAL CODE

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:





Or Visit:  
[\[IDX URL\]](#)

[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 it 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.

As an added precaution we are offering identity theft protection services at no cost to you through IDX, A Zero Fox Company. These services include: [18] months of complimentary credit and Cyberscan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will assist you in resolving issues if your identity is compromised. PLEASE NOTE THAT THE DEADLINE FOR ENROLLMENT IN THIS SERVICE IS \_\_\_\_\_, 2025.

## **WHAT YOU CAN DO**

We encourage you to contact IDX with any questions and to enroll in the offered free identity protection services by calling [TFN], going to <http://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above.

To help protect your personal information, we strongly recommend you take the following steps all of which are good ideas in any event:

- (1) Enroll in the credit monitoring service that we are offering to you. This will enable you to get alerts about any efforts to use your name and social security number to establish credit and restoration assistance if you were not the one who initiated it.
- (2) Review the attached Recommended Steps document providing further information on steps you can take to protect your information.
- (3) Carefully review statements sent to you by your bank, credit card company and other financial and government institutions. Notify the sender of these statements immediately by phone and in writing if you detect any suspicious activity or transactions.

## **MORE INFORMATION**

You will find detailed instructions for enrollment in the enclosed Recommended Steps document. Please reference the enrollment code at the top of this letter when calling or enrolling online. Please call [TEL NUMBER] or go to <http://app.idx.us/account-creation/protect> for any questions you may have.

Sincerely,

E. Baird Archbald  
President

## Recommended Steps to Help Protect Your Information

**1. Website and Enrollment.** Scan the QR image or go to [\[IDX URL\]](#) and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

**2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

**3. 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.

**4. 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](http://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.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that 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.

**5. 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		
<a href="http://www.equifax.com">www.equifax.com</a>			<a href="http://www.experian.com">www.experian.com</a>			<a href="http://www.transunion.com">www.transunion.com</a>		

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.**

**6. 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.

**7. 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](http://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](http://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](http://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](http://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/](http://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](http://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: 1-866-653-4261.