

September 12, 2024

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDtehft@oag.state.md.us

Re: Data Incident Notice – Anderson Feazel Management, Inc.
File No. 21943.3

Dear Attorney General Brown:

My firm has been retained to represent Anderson Feazel Management, Inc. (“Anderson”) in data security matters. Anderson is a Louisiana corporation located at 333 Texas Street, #2020, Shreveport, LA 71101. This correspondence concerns a data breach that affected 26 Maryland residents.

On or around July 31, 2024, Anderson’s computing systems were compromised by a malicious actor who accessed and exfiltrated certain unencrypted documents containing business records, mineral leases, pay records, and other personal information. The personal information that may have been compromised includes names, birth dates, Social Security Numbers, address, salary information, W-2s, and other tax-return documents. Anderson is in the business of oil and gas well investments, so the information compromised of Maryland residents relates to land transactions associated with oil and gas royalties.

Anderson discovered the breach on August 1, 2024. After discovery, Anderson involved local and federal law enforcement and retained computer forensics services to investigate and contain the breach and restore functionality. The security of the information entrusted to Anderson is a top priority, so Anderson is taking further steps to protect itself and consumers from further incident. Anderson has implemented password changes and additional security monitoring and is exploring additional technical and administrative safeguards to further its security program.

Anderson is offering affected consumers 12 months of credit monitoring and identity theft protection services through Equifax. A copy of the notice to be sent to affected persons on September 13, 2024 is included with this letter.

It is our understanding that this correspondence should meet the requirements for notice under the Maryland Personal Information Protection Act. However, if any additional information is required, please do not hesitate to contact me at jessica.engler@keanmiller.com or (504) 620-3361.

September 12, 2024
Page 2

Very truly yours,

KEAN MILLER LLP

Jessica C. Engler

Jessica C. Engler, CIPP/US, CIPM

ANDERSON FEAZEL MANAGEMENT, INC.
333 Texas Street, #2020
Shreveport, LA 71101

September 12, 2024

00695-ADFFIN G0356 L001 AUTO *000003



Notice of Data Breach

Dear Affected Party,

We are sending this letter to you as part of Anderson Feazel Management, Inc.'s ("**Anderson**") commitment to protecting your privacy, security, and confidential information. We take information privacy very seriously, and it is important to us that you are made fully aware of any potential privacy issue. The purpose of this notice is to inform you of an incident that affected Anderson that involved your private or personal information, to provide you with information about the incident, our response to it, and additional steps you may take to better protect your private or personal information, should you feel it appropriate to do so.

What Happened

On or around July 31, 2024, Anderson's computing system was attacked by a malicious actor. Through that attack, the malicious actor accessed and exfiltrated certain unencrypted financial documents that contained individual and employee records, business records, mineral leases, pay records, and other private or personal information. Upon discovery of this intrusion on August 1, 2024, Anderson promptly involved the FBI and state law enforcement and is now providing this notice in accordance with applicable law, guidance from law enforcement, and our investigative efforts.

What Information Was Involved

The personal information that may have been obtained by the third party will depend on your relationship with us and the documents we retain. The personal information may have included: your name, birth date, Social Security Number, address, salary information, W-2s, and tax return documents.

What We Are Doing

Upon discovery, Anderson contacted federal and local law enforcement and took steps to safely restore its systems and operations, including forced password changes and augmented security monitoring. Anderson further engaged an independent subject matter expert for a full forensic investigation to determine the vector of the attack, the nature and scope of the incident, and assist in remediation efforts.

The security and privacy of information contained within Anderson's systems is a top priority, and Anderson is also taking additional measures to protect this information. We are conducting thorough reviews and strengthening of our security systems, including upgraded monitoring and testing, and are taking steps to further implement additional safeguards, policies, and procedures relating to data privacy and security. We are sending you this notice so that you can, in addition to our efforts, act as you see fit to protect your identity. Please see the enclosed "Additional Resources" for additional information.

As part of this effort, Anderson will also be providing you with access to 12 months of credit monitoring and identity protection services through Equifax. This product provides you with identity detection and resolution of identity theft. Please see the enclosed sheet for further information about the Equifax monitoring product and instructions for enrollment.



What You Can Do

Anderson encourages you to remain vigilant against incidents of identity theft and fraud, to monitor your account statements and free credit reports, and to watch for suspicious or unauthorized activity. If you are contacted by the malicious actor, we recommend that you do not engage with this group. If you are aware of or otherwise suspect or discover that your information has been disclosed and/or used inappropriately, please notify your local law enforcement, your state attorney general, or consumer protection agency. For more information on additional steps you can take to protect this information, please see the "Additional Resources" pages that follow this letter and sign up for the offered credit monitoring.

More Information

Should you have any questions or need additional information, including additional information about your personal information maintained by Anderson, please contact Kyle McInnis at (318) 227-2000 or via email at kyle.mcinnis@andersonoilandgas.com.

We take very seriously our role of protecting your private and personal information. Unfortunately, cyberattacks continue to increase at an alarming rate and no organization is completely immune despite the security initiatives taken to prevent such attacks. We have taken and will continue to take steps to maximize our security, minimize the impact of this attack, and prevent a reoccurrence in the future.

Please keep this notice for your records.

Sincerely,

Kyle McInnis

Kyle McInnis
Anderson Feazeal Management, Inc.



Activation Code: [REDACTED]
Enrollment Deadline: **December 31, 2024**

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to **www.equifax.com/activate**

Enter your unique Activation Code of [REDACTED] then click “Submit” and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

¹WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. ²The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. ³Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com ⁴The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



Additional Resources

Order Your Free Credit Report. You are entitled to receive your credit report from each of the three national credit reporting agencies once per year, free of charge. You may obtain your free annual credit report by visiting www.annualcreditreport.com, by calling toll-free at 1-877-322-8228, or completing the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The credit reporting bureaus provide credit reports only through the website, toll-free number, or request form. Do not contact the three credit bureaus individually.

When you receive your credit report, review it carefully. Errors may be a warning sign of potential identity theft. Here are a few tips of what to look for:

- Look for accounts that you did not open.
- Look in the "Inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell if this is the case.
- Look in the "Personal Information" section for inaccuracies in information (such as home address or Social Security Number).

If you see anything you do not recognize, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so that the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity. You have a right to obtain a copy of the police report, which you may need to provide to creditors to clear up your records.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including monitoring your credit reports and account statements.

Fraud Alerts. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file at no cost for 1 year. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit with a fraud alert set, the merchant must take additional steps to verify the identity of the applicant. If you are a victim of identity theft, you are entitled to an extended fraud alert for 7 years.

You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax P.O. Box 105069 Atlanta, GA 30348 800-525-6285 www.equifax.com	Experian P.O. Box 2002 Allen, TX 75013 888-397-3742 www.experian.com	TransUnion P.O. Box 2000 Chester, PA 19022-2000 800-680-7289 www.transunion.com
---	--	---

Security Freeze. You have the right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. Please be aware that using a security freeze to control who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request of application you make regarding a new loan, credit, mortgage, or other account involving the extension of credit.

You can place, temporarily lift, or permanently remove a security freeze on your credit report online, by phone, or by mail. You will need to provide certain personal information, such as address, date of birth, Social Security number, proof of current address, or copy of state-issued identification card to request a security freeze and may be provided with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. Information on how to place a security freeze with the credit reporting agencies is also contained in the links below:

<https://www.equifax.com/personal/credit-report-services/>
<https://www.experian.com/freeze/center.html>
<https://www.transunion.com/credit-freeze>

As of June 30, 2023, the credit bureaus allow you place a credit freeze through online, physical mail, and phone numbers, and request that you provide the information listed below. Where possible, please consult the websites listed above for the most up-to-date instructions.

Reporting Agency	Online	Physical Mail	Phone Number
Equifax	Freeze request may be submitted via your myEquifax account, which you can create here: https://my.equifax.com/consumer-registration/UCSC/##personal-info	The Equifax Freeze Request Form may be found here: https://assets.equifax.com/assets/personal/Security_Freeze_Request_Form.pdf and mailed to: Equifax Information Services LLC P.O. Box 105788 Atlanta, GA 30348-5788	888-298-0045
Experian	Freeze request may be submitted here: https://www.experian.com/ncaconline/freeze	Mail the request to: Experian Security Freeze P.O. Box 9554 Allen, TX 75013	888-397-3742
TransUnion	Freeze request may be submitted via your TransUnion account, which you can create here: https://service.transunion.com/dss/orderStep1_form.page?	Mail the request to: TransUnion P.O. Box 160 Woodlyn, PA 19094	888-909-8872

Fees associated with placing, temporarily lifting, or permanently removing a security freeze no longer apply at nationwide consumer reporting agencies.

Additional Information. Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the FTC, or their state attorney general. The FTC may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The FTC also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement. A checklist of the steps listed above and links to forms and other helpful information can be found on the site at <https://IdentityTheft.gov/steps>

Federal Trade Commission and State Attorneys General Offices. If you believe that you are the victim of identity theft or have reason to believe that your personal information has been misused, you should immediately contact local law enforcement authorities, the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.



You may contact the **Federal Trade Commission** to learn more about how to protect yourself from identity theft at Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For Connecticut Residents: You may contact the Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

For District of Columbia Residents: You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General, 441 4th Street, NW, Washington, DC 20001, 202-442-9828, www.oag.dc.gov

For Maryland Residents: You may contact the Maryland Attorney General's Office, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, <https://www.marylandattorneygeneral.gov/>

For Massachusetts Residents: You may contact the Office of the Attorney General, One Ashburton Place, 18th Floor, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

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

For New York Residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224, 1-800-771-7755, <https://ag.ny.gov> You may also contact the New York Department of State Division of Consumer Protection, 99 Washington Avenue, Ste. 650, Albany, NY 12231, 1-800-697-1220, www.dos.ny.gov

For North Carolina Residents: You may contact the North Carolina Attorney General's Office, 9001 Mail Service Centre, Raleigh, NC 27699-9001, 1-919-716-6000, 1-877-566-7226, www.ncdoj.gov

For Oregon Residents: We encourage you to report suspected identity theft to the Oregon Attorney General at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

For Rhode Island Residents: You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov For security incidents generally, you have the right to obtain a copy of a police report. This incident impacted 3 Rhode Island residents.

Reporting Identity Theft and Obtaining a Police Report.

For Iowa Residents: You are advised to report any any suspected identity theft to law enforcement or to the Iowa Attorney General. The Iowa Attorney General may be contacted at Office of the Iowa Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, 515-281-5926, 888-777-4950, www.iowaattorneygeneral.gov

For Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection with the 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.

For Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's office at: 800-649-2424 (toll-free in Vermont), 802-656-3183.

For West Virginia Residents: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.