



RECEIVED

OCT 19 2021

Anjali C. Das

312.821.6104 (direct)

CONSUMER PROTECTION

Anjali.Das@wilsonelser.com

October 13, 2021

CONFIDENTIAL

Via: First Class Mail

John Formella
Office of Attorney General of New Hampshire
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Cybersecurity / Data Privacy Incident
Client: PetroQuest Energy LLC
File No.: 15991.00979

Dear Attorney General Formella:

Wilson Elser represents PetroQuest Energy LLC “PetroQuest” an independent energy company engaged in the exploration, development, acquisition and production of oil and natural gas reserves in Texas and Louisiana. PetroQuest was impacted in a cybersecurity incident that compromised an employee’s business email account. This letter contains more information about the incident and steps PetroQuest has taken in response.

1. Nature of the incident.

On April 9, 2021, PetroQuest discovered unauthorized access to its systems that may have resulted in access to personally identifiable information (“PII”). After learning about the potential unauthorized access, PetroQuest engaged a forensic team to review the impacted system in order to learn more about the scope and extent of the incident, and whether PII may have been exposed. The forensic investigation confirmed that an unauthorized individual had access to our systems between March 13, 2021 and April 9, 2021.

The forensic investigation determined that some files on PetroQuest’s systems may have been accessed by the unauthorized individual. The investigation did reveal that the bad actor may have had access to PetroQuest’s Quorum database which contains landowner and lease agreements. Notably, much of the information contained in the lease agreements are public record. However, certain older files containing lease agreements and lease packets may have included individuals’ W-9s with their taxpayer ID or social security number. Given the size and age of the database, PetroQuest had to manually review its records dating back many years to identify potentially

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

affected individuals. This exercise was completed by PetroQuest on September 23, 2021.

2. Number of New Hampshire residents affected.

5 New Hampshire resident(s) were potentially affected by this incident. Incident notification letters were mailed out on October 15, 2021 via First Class Mail. A sample copy of the Incident notification letter mailed to potentially affected resident(s) is included with this letter at **Exhibit A**.

3. Steps taken.

At this time, there is no evidence that any information has been misused as a result of this incident. PetroQuest has taken steps to further safeguard data in the future - including but not limited to updating existing firewalls, removing all public facing servers from the network, implementing stronger AV and EDR software, replacing remote connection software with a version that supports MFA, improving offsite backup testing, and requiring MFA for admin accounts. PetroQuest is also offering complimentary credit monitoring to the affected individuals.

4. Contact information.

PetroQuest remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

Enclosure

EXHIBIT A

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Allentown • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com



Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Dear <<Name 1>>:

Notice of Data Breach:

PetroQuest Energy LLC "PetroQuest" is writing to inform you of a recent cybersecurity incident that may have involved some of your personal information. This letter contains details about the incident, steps we have taken in response and services we are making available to you.

What happened?

On April 9, 2021, PetroQuest discovered unauthorized access to its systems that may have resulted in access to your personally identifiable information ("PII"). After learning about the potential unauthorized access, PetroQuest engaged a forensic team to review the impacted system in order to learn more about the scope and extent of the incident, and whether PII may have been exposed. The forensic investigation confirmed that an unauthorized individual had access to our systems between March 13, 2021 and April 9, 2021.

What information was involved?

The forensic investigation determined that some files on our systems may have been accessed by the unauthorized individual. The investigation was not able to definitively conclude what information stored on our systems, if any, was in fact accessed by the bad actor. However, the investigation did reveal that the bad actor may have had access to PetroQuest's Quorum database which contains landowner and lease agreements. Notably, much of the information contained in the lease agreements are public record. However, certain older files containing lease agreements and lease packets may have included individuals' W-9s with their taxpayer ID or social security number. While there is no evidence that the bad actor actually accessed, copied, archived, exfiltrated, or misused imaged files contained in this database, PetroQuest is nonetheless notifying individuals of this incident out of an abundance of caution. Given the size and age of the database, PetroQuest had to manually review its records dating back many years to identify potentially affected individuals. This exercise was completed by PetroQuest on September 23, 2021.

What we are doing and what can you do:

PetroQuest takes the security of your personal information very seriously, and has taken steps to prevent a similar event from occurring in the future. In order to help relieve concerns and restore confidence following this incident, we are offering you access to credit monitoring and identity theft protection services for 12 months at no cost to you, through Equifax. You may find information on how to enroll in these services in the enclosed "Steps You Can Take to Help Protect Personal Information."

Other Important Information:

The protection of your information is a top priority, and we sincerely regret any concern or inconvenience that this incident may cause you. We remain dedicated to maintaining the security and protection of your information and have responded to this incident as follows: updating existing firewalls, removing all public facing servers from the network, implementing stronger AV and EDR software, replacing remote connection software with a version that supports MFA, improving offsite backup testing, and requiring MFA for admin accounts.

We encourage you to remain vigilant and review the enclosed addendum outlining additional steps you can take to protect your personal information. If you have any questions or want to enroll in the complimentary identity monitoring services, please call 1-800-601-9089, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

400 E. Kaliste Saloom Rd., Suite 3000 • Lafayette, Louisiana 70508

AE7291 v.02

P.O. Box 51205 • Lafayette, Louisiana 70505-1205 • (337) 232-7028 • Fax (337) 232-0044

Steps You Can Take to Help Protect Personal Information

Enroll in Equifax Credit Watch Gold



Enter your Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<Enrollment Deadline>>

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 <<ACTIVATION CODE>> 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.

¹ WebScan 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.

⁴ The 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.