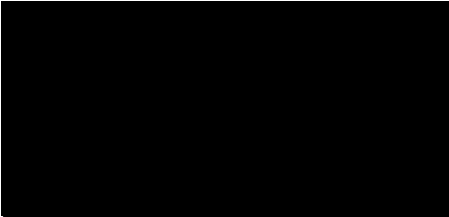




May 27, 2016



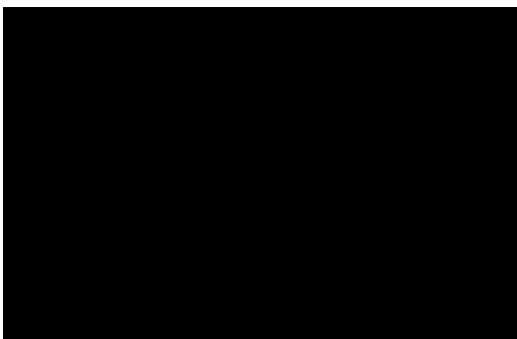
Extraction Oil & Gas, LLC ("Extraction") has learned of an inadvertent disclosure of the personal information of some of our present and former employees. This disclosure occurred on May 23, 2016, as a result of a phishing scam where an email was sent that appeared to be from an employee and it was not in fact from that person. The email requested copies of the W-2 forms for all Extraction employees for 2015. The forms for all present and former employees were emailed in response to the phishing scam. As a result of this inadvertent disclosure, your name, address, Social Security number and wage amounts for 2015 were released. We identified the inadvertent disclosure on Tuesday, May 24, 2016. We have notified the Denver Police Department and filed a police report (Denver Police Case Number 2016-5002054). We are notifying you so that preventative action is taken to minimize or eliminate any potential harm. We understand that this may be stressful, but we are here to help because we take the protection of your personal information very seriously. Please contact me if you have any questions or if I can help you through this process.

As a result, we have retained ID Watchdog Inc. to provide identity monitoring, identity theft detection, and resolution services to all employees free of charge as an additional employee benefit. This program monitors thousands of public and private databases for new and updated information associated with your personal, identifiable and financial information, among other services. You will receive a letter under separate cover with the free enrollment information. If you have any difficulties enrolling, please call me at (720) 481-2363.

We have reported this inadvertent disclosure to the State of Montana Attorney General's Office of Consumer Protection, as required by law since you are a Montana resident. Your identity has not been disclosed to the Attorney General.

The additional information enclosed in this letter details the steps Extraction has taken and the additional steps we suggest you take to protect yourself in light of this incident.

If you have any further questions, please do not hesitate to contact me at (720) 481-2363. We apologize for any inconvenience or concern this may raise and we are here to help you through this process.



Recommended Steps to Ensure Identity Protection

We recommend that you closely monitor your financial accounts. If you see any unauthorized activity, promptly contact your financial institution and submit a complaint to the Federal Trade Commission ("FTC") by calling 1-877-ID-THEFT (1-877-438-4338), or online at <https://www.ftccomplaintassistant.gov/>. You may wish to review the tips provided by the FTC on how to avoid identity theft. For more information, please visit <http://www.ftc.gov/idtheft> or call the number listed above.

You should also contact the three major U.S. consumer reporting agencies, which are Equifax, Experian, and TransUnion to obtain a free credit report from each company by calling 1-877-322-8228 or visiting www.annualcreditreport.com. The Federal Trade Commission recommends that you check your credit report periodically, even if you do not find any suspicious activity on the initial credit report. You may want to obtain your credit report from each of the three bureaus again within 60-90 days from obtaining the first report. A victim's personal information is sometimes held for later use or is shared among groups of thieves. Checking your credit report periodically will help you identify problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, contact your local law enforcement agency and file a police report. Since the phishing scam occurred in Denver, you can report the crime quickly by using the Denver Police Department online form at www.denvergov.org/policerreport. You should obtain and keep a copy of the police report; many creditors will require the information contained in the police report to absolve you any fraudulent debts. Extraction filed a police report on behalf of the company; however, you must individually file a report if your personal information is used fraudulently. You should also file a complaint with the FTC at <https://www.ftccomplaintassistant.gov/>. You can also complete an Identity Theft Passport application through the Montana State Department of Justice's Office of Consumer Protection and return it to the law enforcement agency listed above at <https://media.dojmt.gov/wp-content/uploads/X-200-Identity-Theft-Passport-Application.pdf>.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, contact your local law enforcement agency and file a police report. Obtain a copy of the police report; many creditors will require the information contained in the police report to absolve you of the fraudulent debts.

If you suspect that someone is using your Social Security number to obtain credit or employment, contact the Social Security Administration's fraud hotline at 1-800-269-0271.

We recommend placing a fraud alert on your credit report. 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 one of the nationwide consumer reporting agencies at the following numbers:

Equifax- 800-525-6285
Experian- 888-397-3742
TransUnion- 800-680-7289

As soon as one consumer reporting agency confirms your fraud alert, it must notify the others. An initial fraud alert is free if you are a victim of identity theft and will stay on your credit file for at least 90 days.

You may obtain a credit or security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge, except as provided by law. You have a right to place a security freeze on your credit report to prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval, except as the law allows.

To place a security freeze on your credit files, you will need to contact the three U.S. consumer reporting agencies separately in order to place a security freeze by (1) making a request in writing by regular or certified mail to a credit reporting agency; or (2) making a request to the consumer reporting agency through a secure electronic mail connection, specified by the consumer reporting agency.

Pursuant to Montana Law, as a Montana consumer you have the right to obtain a security freeze on your credit report to protect your privacy.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval, except as otherwise allowed by law.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. Generally, a consumer reporting agency shall place a security freeze on a credit report within five (5) days after receiving a written or electronic request with proper identification and fee, if applicable. A consumer reporting agency shall place a security freeze within twenty-four (24) hours of a request from a victim of identity theft that requests a security freeze and provides a valid police report, investigative report, or complaint that the consumer has filed with a law enforcement agency.

When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number, password, or other device to use if you choose to remove the security freeze on your credit report or to temporarily authorize the release of your credit report for a specific party, parties, or period of time after the security freeze is in place. To provide that authorization, you shall contact the consumer reporting agency and provide all of the following: (1) the unique personal identification number, password, or other device provided by the consumer reporting agency; (2) the proper identification to verify your identity; (3) the proper information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report is to be available to users of the credit report; and (4) a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to temporarily lift a security freeze on a credit report shall comply no later than three (3) business days after receiving the request in writing or within fifteen (15) minutes of receiving a request by telephone or through a secure electronic connection. After receiving a request from the consumer to remove a security freeze, a consumer reporting agency shall remove the security freeze within three (3) business days of receiving a removal request at the point of contact designated by the consumer reporting agency if the consumer provides the proper identification; and the unique personal identification number, password, or other device provided by the consumer reporting agency.

Generally, a consumer reporting agency may not charge a consumer who has been the victim of identity theft and who has submitted to the consumer reporting agency a valid police report, an investigative report, or a complaint that the consumer has filed with a law enforcement agency or to permanently remove the freeze. A consumer reporting agency may charge an administrative fee of three dollars (\$3.00) or less, to a consumer to place or temporary lift a security freeze. A consumer may be charged a reasonable fee of five dollars (\$5.00) or less, if the consumer fails to retain the original personal identification number, password, or other device provided by the consumer reporting agency and if the consumer asks the consumer reporting agency to reissue the same or a new personal identification number, password, or other device.

A security freeze does not apply to circumstances in which you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, or similar activities.

You should be aware that using a security freeze to control access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding new loans, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular phone, utilities, digital signature, internet credit card transaction, or other services, including an extension of credit at the point of sale. If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around, or specifically for a certain creditor, a few days before actually applying for new credit.

To place a security freeze, either use each consumer reporting agency's online process or send a letter by regular or certified mail to each of the three consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
<https://www.freeze.equifax.com/>

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/freeze/>

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19022
<https://www.transunion.com/freeze>

To place the security freeze with each consumer reporting agency, you may be asked to:

- provide your full name (including middle initial as well as Jr., Sr., II, III, etc.), address, Social Security number, and date of birth;
- provide your addresses where you have resided over the prior five years, if you have moved in the past five years;

May 27, 2016

Page 5

- provide proof of current address such as a current utility bill or phone bill (alternative options include a bank, insurance, or credit card statement listing your full name and address); and
- provide a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.).