Kennedys

1600 Market Street
Suite 1410
Philadelphia, PA 19103
USA

t +1 267.479.6700
f +1 215.665.8475

kennedyslaw.com

t +1 267 479 6706
Joshua.Mooney@kennedyslaw.com
March 12, 2025

By WEB FORM

Attorney General Nicholas W. Brown
Office of the Attorney General
800 Fifth Avenue
Suite 2000
Seattle, WA 98104

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Kennedys CMK, LLP ("Kennedys") represents Trinity Petroleum Management, LLC ("Trinity Petroleum Management"), an accounting service provider located in Denver, Colorado.

We write to provide notice to your office of a data security incident potentially impacting the personal information of 748 Washington residents as required by Wash. Rev. Code §§ 19.255.005–.040C.

I. Nature of Security Incident

On October 14, 2024, Trinity Petroleum Management became aware of technical issues related to systems in its network. Upon discovery, Trinity Petroleum Management took immediate action to secure its network and to address and investigate the incident. This included retaining legal counsel and engaging outside IT forensic specialists (at the direction of counsel) to investigate. After a thorough forensic investigation, on December 18, 2024, Trinity Petroleum Management learned that an unauthorized actor gained access to Trinity Petroleum Management's systems from October 10, 2024 to October 14, 2024, and may have exfiltrated data, including some personal information.

II. Affected Washington Residents

Trinity Petroleum Management notified 748 state residents via U.S. mail in two waves that occurred on February 13, 2025 and March 10, 2025, respectively. The impacted data varied by individual but included individuals' names, Social Security numbers, and financial account information. Notified individuals were offered an opportunity to enroll in 12 months of complimentary credit monitoring and identity protection services through TransUnion. Trinity

Petroleum Management also set up a dedicated call center to respond to notified individuals' inquiries on the incident and assist with enrollment in credit monitoring services. A sample copy of the notification letter is enclosed.

III. Steps Taken in Response to the Incident

Trinity Petroleum Management has taken steps in response to the incident to help mitigate the risk of a similar incident occurring in the future, such as initiating a mandatory global password reset and implementing multi-factor authentication protocols for employees and clients. Existing end point detection tools were supplemented by bespoke detection and response monitoring tools to further strengthen the security of Trinity Petroleum Management's systems. Trinity Petroleum Management is also implementing 24/7 third-party monitoring, management, remediation, and reporting of all end point detection response activity. Trinity Petroleum Management also notified law enforcement of the incident.

Should you have any further questions, please do not hesitate to contact me. Thank you.

Very truly yours,

/s/Joshua A. Mooney

Joshua A. Mooney

Partner
for Kennedys

Enclosures: Sample Individual Notification Letter

Trinity Petroleum Management, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

P
[redacted]

TRINITY PETROLEUM MANAGEMENT, LLC
1670 Broadway, Suite 2000, Denver, Colorado 80202
Telephone (303) 296-1908

February 13, 2025

Re: ***Notice of Data Security Breach***

Dear [redacted]:

We are writing to inform you of a data security breach experienced by our company that may have involved your personal information. We take privacy and security very seriously. This notice explains the incident, steps our company has taken to address it, and provides guidance on steps you can take to help protect your personal information. We also provide below the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened

On October 14, 2024, we learned of an unauthorized access to our systems. Upon detection, we took immediate action to terminate further access and investigate the incident. We retained legal counsel and engaged external cybersecurity forensic specialists to conduct an investigation.

As part of the investigation, we identified the impacted systems and performed a detailed review of the contents to determine the data that may have been impacted and to whom that information relates. After a thorough investigation, we determined that an unauthorized actor gained access to our systems between October 10 and October 14, 2024. On December 18, 2024, we determined that your data may have been exfiltrated.

What Information Was Involved

The information that may have been impacted includes your first and last name, in combination with your Social Security number.

What We Are Doing

Prior to the incident, Trinity Petroleum Management had a number of security measures in place. Upon learning of the incident, we implemented additional security safeguards. We retained legal counsel and engaged outside forensic specialists (via counsel) to assist with evaluating the incident as outlined above. We also notified law enforcement.

Additionally, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no cost to you. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Instructions about how to enroll in these services and additional resources available to you are included in the enclosed "*Steps You Can Take to Help Protect Your Information*."

000010102G0400

P

What You Can Do

As a general matter, it is prudent to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft, as well as credit monitoring enrollment instructions.

For More Information

Should you have any questions or concerns, please contact our dedicated assistance line at 1-833-799-4205, Monday through Friday between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, excluding major U.S. holidays. Please know that the security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support during this time.

Sincerely,

J. Samuel Butler
President
Trinity Petroleum Management, LLC

Enclosure: *Steps You Can Take to Help Protect Your Information*

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

How do I enroll for the free services?
To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts and Credit Reports:
We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors.

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Fraud Alert Services:
You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

Credit Freeze Instructions:
As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

0000102028000 P

TransUnion 1-833-806-1627 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-378-4329 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them.

The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and https://oag.dc.gov/consumer-protection.

For Maryland residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.marylandattorneygeneral.gov.

For Kentucky residents, the Kentucky Attorney General may be contacted at 700 Capitol Avenue, Suite 118, Frankfurt, Kentucky 40601; 502-696-5300; and www.ag.ky.gov.

For New Mexico residents, you have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit:
https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Oregon residents, the Oregon Attorney General may be contacted at Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096; 1-877-877-9392; and https://doj.state.or.us/consumer-protection/.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 12 Rhode Island residents whose data is impacted by this incident.