



Gregory R. Schermerhorn
Senior Counsel

Marathon Petroleum Company LP

539 South Main Street
Findlay, Ohio 45840
Tel: 419.421.4203
grschermerhorn@marathonpetroleum.com

RECEIVED

APR 15 2019

CONSUMER PROTECTION

April 8, 2019

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Security Breach as required by the New Hampshire Data Breach Notification Law

Dear Sir or Madam:

I am the attorney for Marathon Petroleum Company LP (“MPC”). This letter serves as MPC’s notice of a security breach (the “Data Breach”) to the Consumer Protection Bureau of the New Hampshire Office of the Attorney General, as required by New Hampshire’s data breach notification law (the “Law”). As required by the Law, MPC provides the following information concerning the Data Breach to the Attorney General.

A. How the Data Breach occurred:

Between November 28, 2018 and March 8, 2019, MPC mistakenly posted to its employee benefits website mympcbenefits.com a copy of IRS Form 8955-SSA for 2017 which contained the Social Security number and the first name, middle initial (if applicable), and last name of certain former employees of MPC. Note that Form 8955-SSA is a confidential form that MPC is required to file with the IRS each year to report retirement plan participants who have terminated employment and who may be entitled to a future retirement benefit.

MPC’s records indicate that the website link for this form was accessed on five occasions. MPC believes that the link was accessed by MPC employees, but it has not been able to actually determine who (internally or externally) accessed the link or whether any information contained on the Form 8955-SSA was downloaded or copied or has since been misused.

B. How many New Hampshire residents were affected:

Two New Hampshire residents – [REDACTED] – were affected by the Data Breach.

C. Sample notification letter:

For your reference, a sample notification letter is attached. Please note that the letter is generic and uses an April 2, 2019 placeholder date and a Florida placeholder address for the affected individual. **For the**

April 11, 2019

Page 2

New Hampshire residents who were affected by the Data Breach, their addresses of record were used and the notification letter was mailed to the affected individuals on April 8, 2019.

D. Other information:

MPC takes its data protection responsibilities seriously and has acted in prompt good faith to address the Data Breach. The posted information was removed from its website upon MPC's learning of the Data Breach, and the affected individuals are being offered free credit monitoring services and explained in the sample notification letter.

If you need any additional information, please do not hesitate to contact me.

Sincerely yours,



Gregory R. Schermerhorn
Senior Counsel

Enclosures



April 2, 2019

FIRST NAME LAST NAME
123 ANY ST
APT ABC
CITY, FL 12345

NOTICE OF DATA BREACH

Dear FIRST NAME LAST NAME,

We are contacting you about a data breach that occurred at Marathon Petroleum Company LP (Company).

What Happened?	<p>Between November 28, 2018 and March 8, 2019, the Company mistakenly posted to its employee benefits website mympcbenefits.com a copy of IRS Form 8955-SSA for 2017 which contained your Social Security number and your first name, middle initial (if applicable), and last name. Form 8955-SSA is a confidential form that the Company is required to file with the IRS each year to report retirement plan participants who have terminated employment and who may be entitled to a future retirement benefit.</p> <p>The Company's records indicate that the website link for this form was accessed on five occasions. The Company does not know who accessed the link or whether any information contained on the Form 8955-SSA was downloaded or copied or has since been misused.</p>
What Information Was Involved?	<p>This incident involved only your Social Security number and your name.</p> <p>The Company maintains this information, because it is necessary for the administration and tax reporting of you Company retirement benefit.</p>

D4CT
000001



What We Are Doing

On March 8, 2019, we permanently removed the Form 8955-SSA from our employee benefits website. It is no longer available on any Company website. We have also reviewed and improved our internal data protection procedures to make sure this situation does not recur.

Additionally, the Company has arranged with Identity Guard® to provide you with credit monitoring for one year, at no cost to you. The credit monitoring provides you with a free one-year subscription to Identity Guard® Total Protection®, a credit monitoring and identity theft protection service. Identity Guard® provides essential monitoring and protection of not only credit data, but also monitors Internet chat rooms and newsgroups and alerts you if your Social Security number, credit cards, and bank account numbers are found in unsecure online locations. This program is provided by Intersections Inc., a leading provider of consumer and corporate identity risk management services.

Identity Guard® Total Protection® features include:

- Social Security Number Monitoring
- Online "Black Market" Monitoring
- Account Takeover Alerts
- Address Change Monitoring
- 3-Bureau Credit Monitoring
- 3-Bureau Credit Reports and Scores*
- \$1 Million Identity Theft Insurance**
- Public Records Monitoring
- Lost Wallet Protection
- And More

To take advantage of this free credit monitoring benefit, you must enroll by

██████████

To activate this coverage please visit the Web site listed below and enter the redemption code. The redemption code is required for enrollment and can only be used one time by the individual addressed.

1. Website: www.identityguard.com/enroll
2. Enter Redemption Code: ██████████ and click "Submit"
3. Complete the Identity Guard® Total Protection® enrollment form. To see additional product features, click "Service Details."

In order to enroll, you will need to provide the following personal information:

- Mailing Address
- Phone Number
- Social Security Number
- Date of Birth
- E-Mail Address
- Redemption Code

The service is complimentary; no method of payment will be collected during enrollment and there is no need to cancel. We apologize for any inconvenience and urge you to enroll today.

**The scores you receive with Identity Guard® are provided for educational purposes to help you understand your credit. They are calculated using the information contained in your Equifax, Experian and TransUnion credit files. Lenders use many different credit scoring systems, and the scores you receive with Identity Guard are not the same scores used by lenders to evaluate your credit.*

Credit scores are provided by CreditXpert® based on data from the three major credit bureaus.

**Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

D4CT
000001



What You Can Do

Remain vigilant by reviewing your various account statements and by monitoring your free credit reports.

You can obtain information from the Federal Trade Commission (FTC) and the credit bureaus about fraud alerts and security freezes.

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days.

Equifax:
Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
1-800-525-6285
security.dataadministration@equifax.com

Experian:
Consumer Fraud Assistance
P.O. Box 9556
Allen, TX 75013
1-888-397-3742
businessrecordsvictimassistance@experian.com

TransUnion:
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
transunion.com/customer-support/contact-us-consumers

Request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report. Get a copy of the police report; you may need it to clear up the fraudulent debts.

If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

You also may want to consider contacting the major credit bureaus at the telephone numbers above to place a credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identify thief can open new accounts in your name. The cost to place and lift a freeze depends on state law. Find your state Attorney General's office at naag.org to learn more.

Finally, you may contact your local police department or your state Attorney General's office to report suspected incidents of identity theft.

DACT
000001



<p>Other Important Information</p>	<p>Visit the FTC's site at IdentityTheft.gov to get a copy of Identity Theft: A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft.</p> <p>Also, because the data breach here involved Social Security number information, the FTC indicates that you should:</p> <ul style="list-style-type: none"> • Take advantage of the free credit monitoring benefit provided by the Company. • Get your free credit reports from annualcreditreport.com. Check for any accounts or charges you don't recognize. • Consider placing a credit freeze. A credit freeze makes it harder for someone to open a new account in your name. • If you place a freeze, be ready to take a few extra steps the next time you apply for a new credit card or cell phone, or any service that requires a credit check. • If you decide not to place a credit freeze, at least consider placing a fraud alert. • Try to file your taxes early, before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. • Respond right away to letters from the IRS. • Don't believe anyone who calls and says you'll be arrested unless you pay for taxes or debt, even if they have part or all of your Social Security number, or they say they're from the IRS. • Continue to check your credit reports at annualcreditreport.com. You can order a free report from each of the three credit reporting companies once a year. <p>In additional to the FTC website above, you may contact the FTC toll-free at 1-877-438-4338 or TTY 1-866-653-4261, or at the following address: Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580.</p>
<p>For More Information</p>	<p>Call 1-888-421-2199 Monday through Friday during normal business hours if you have questions about the data breach or the information contained in this letter.</p> <p>If the Company learns of any additional information regarding this data breach that may affect you, we will contact you at your address of record. Please notify us if your address changes.</p>

D4CT
000001



Sincerely,

R. K. Mattingly
On behalf of
Marathon Petroleum Company LP