

RECEIVED

AUG 01 2017

CONSUMER PROTECTION

 **NORTON ROSE FULBRIGHT**

Norton Rose Fulbright US LLP

1301 Avenue of the Americas
New York, New York 10019-6022
United States

Direct line +1 212 318 3105
boris.segalis@nortonrosefulbright.com

Tel +1 212 318 3000
Fax +1 212 318 3400
nortonrosefulbright.com

July 26, 2017

**By Certified Mail
Return Receipt Requested**

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, Delek US Holdings, Inc. ("Delek"), to inform you of a security incident involving personal information that affected approximately 7 New Hampshire residents. Delek is notifying these individuals and outlining some steps they may take to help protect themselves.

On May 23, 2017, an unknown person broke into the vehicle of a Delek employee. The criminal stole various items from the employee's vehicle, including a Delek-issued laptop computer. The theft was reported to law enforcement on the day of the incident, but to date the laptop has not been recovered.

Delek had implemented various security protections on the laptop, but it cannot guarantee that these protections are incapable of being circumvented. Delek did not have a recent backup image of the computer, so it conducted an investigation into the files that could have been stored on the computer. On June 26, 2017, Delek discovered it was possible that certain files containing personal information may have been stored on the laptop, including some that may have included individuals' names, addresses, compensation and benefits information, and/or Social Security numbers.

Delek takes the privacy of personal information seriously and deeply regrets that this incident occurred. It is reviewing and updating its information security policies and practices to add additional safeguards for personal information. Delek is also notifying affected individuals via written letter, which includes an offer of one year of complimentary identity protection and fraud resolution services. These notifications will begin mailing on or around July 26, 2017. A form

Norton Rose Fulbright US LLP is a limited liability partnership registered under the laws of Texas.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients. Details of each entity, with certain regulatory information, are available at nortonrosefulbright.com.

Office of the New Hampshire Attorney General
July 26, 2017
Page 2

NORTON ROSE FULBRIGHT

copy of the notice being sent to affected New Hampshire residents is included for your reference.

If you have any questions or need further information regarding this incident, please contact me at (212) 318-3105 or boris.segalis@nortonrosefulbright.com.

Very truly yours,

A handwritten signature in black ink, appearing to read "Boris Segalis". The signature is fluid and cursive, with a large initial "B" and a long, sweeping tail.

Boris Segalis
Partner

BS
Enclosure



Delek US Holdings, Inc.
7102 Commerce Way
Brentwood, TN 37027

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

<<Date>> (Format: Month Day, Year)

Dear <<MemberFirstName>> <<MemberLastName>>,

Delek US Holdings, Inc. ("Delek") recently became aware of a security incident that may have affected the personal information of certain current and former employees; and, in some instances, their spouses, beneficiaries, and dependents. We are providing this notice as a precaution to inform potentially affected individuals of the incident and to call their attention to some steps they can take to help protect themselves. We sincerely regret any concern this incident may cause you.

What Happened?

On May 23, 2017, an unknown person broke into the vehicle of a Delek employee. The criminal stole various items from the employee's vehicle, including a Delek-issued laptop computer. The theft was reported to law enforcement on the day of the incident, but to date the laptop has not been recovered. Various security protections were in place on the laptop, but we cannot guarantee that these protections are incapable of being circumvented.

What Information Was Involved?

The laptop contained various files that may have included your name, address, Social Security number, and/or information about compensation and benefits. We want to stress that we are not aware of any unauthorized access, fraud or misuse of your information as a result of this incident, and we are providing this notice out of an abundance of caution.

What We Are Doing

We take the privacy of personal information seriously and deeply regret that this incident occurred. We are reviewing and updating our information security policies and practices to add additional safeguards for your personal information. We have also engaged Kroll to provide identity monitoring services at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. This service helps detect possible misuse of your personal information and provides you with support focused on identification and resolution of identity theft. For more information about these services and instructions on activating the services, please refer to the "Information about Identity Theft Protection" reference guide attached to this letter.

As indicated above, law enforcement has been notified, and we will continue to assist them in an effort to identify and find those responsible for the theft.

What You Can Do

We want to make you aware of steps you can take to guard against fraud or identity theft. You should carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit

DELEK REFINING * DK CANADA * DELEK LOGISTICS PARTNERS * LION OIL COMPANY

reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records.

You should also regularly review financial account statements. We urge you to remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should immediately notify the relevant institution.

As an additional precaution, we are providing information and resources to help individuals protect their identities. This includes an "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection.

For More Information

If you have additional questions or concerns about this incident, you may contact us at 1-877-309-9839 Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Again, we are sorry for any inconvenience or concern this event may cause you.

Sincerely,



Mark Davison
Chief Information Officer

INFORMATION ABOUT IDENTITY THEFT PROTECTION

Identity Monitoring Services Activation Instructions:

We have retained Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

To activate and take advantage of your identity monitoring services, visit my.idmonitoringservice.com.

*You have until **11/2/2017** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-877-309-9839. Additional information describing your services is included with this letter.

Review Accounts and Credit Reports: As a precaution, you may regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, <http://www.riag.ri.gov>.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed below.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)

P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:

https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp

Credit Freezes:

<https://www.freeze.equifax.com>

Experian (www.experian.com)

P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts:

<https://www.experian.com/fraud/center.html>

Credit Freezes:

https://www.experian.com/consumer/security_freeze.htm

TransUnion (www.transunion.com)

P.O. Box 1000
Chester, PA 19016
800-888-4213

Fraud Alerts:

<http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page>

Credit Freezes:

<http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page>



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher. Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona. Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan. Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement. Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.