

RECEIVED

JUN 17 2019

CONSUMER PROTECTION

June 14, 2019

William Sanders
214-698-8063 (direct)
William.Sanders@wilsonelser.com

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Data Security Incident

Dear Attorney General MacDonald:

We represent Energy United with respect to an incident involving the potential exposure of certain personal information described in detail below.

1. Nature of the possible security breach or unauthorized use or access

In February and March of 2019, Energy United was the target of a cyber-attack which affected two (2) of its employees' accounts. Energy United immediately conducted a forensic investigation to determine the scope and extent of the incident, pursuant to which it was determined that banking information of a New Hampshire resident may have been compromised. Energy United has no evidence to suggest that any personal information is being misused at this time.

2. Number of New Hampshire residents potentially affected

Approximately one (1) New Hampshire resident was affected in this potential incident. Energy United is sending the potentially impacted individual a letter notifying them of this incident. A copy of the notification sent to the potentially impacted individual is included with this letter, which informs this New Hampshire resident about the 12 months of credit monitoring and identity theft protection services that is being offered to them.

3. Steps Energy United has taken or plans to take relating to the potential incident

Energy United has taken steps to prevent a similar event from occurring in the future, including reviewing its information, security policies and procedures, and implementing additional safeguards to protect against this threat by storing all data in a new secure environment.

4. Anticipated date of disclosure

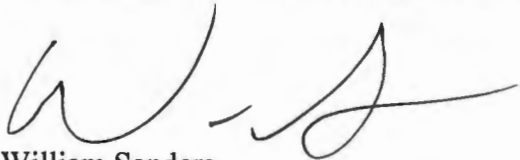
Energy United began mailing letters to approximately one New Hampshire resident pursuant to the requirements of the Health Insurance and Portability Act ("HIPAA"), 45 C.F.R. §§164.400-414 and state law in substantially the same form as the letter attached hereto.

5. Other notification and contact information

If you have any additional questions, please contact me at William.Sanders@wilsonelser.com, or by phone at (214) 698-8063.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



William Sanders
Counsel

Enclosure



Return Mail Processing Center
PO Box 9349
Dublin, Ohio 43017

<<Mail ID>>
<<Name >
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>>

June 14, 2019

Dear <<Name>>,

We are writing to inform you of a cyber-attack which compromised an email password at EnergyUnited which may have exposed your banking information. We take the security of your personal information seriously and want to provide you with information and resources you can use to protect your information.

WHAT HAPPENED

In February and March of 2019, we believe that two (2) employee accounts were the target of a cyber-attack. We immediately engaged Ankura, a leading global forensic firm, to support our investigation into this activity. The investigation revealed that your banking information may have been compromised pursuant to this incident. While we have no evidence to suggest that any of your sensitive personal information is being misused, we wanted to make you aware of the event out of an abundance of caution.

WHAT WE ARE DOING

In light of this incident, we have taken steps to prevent this from happening in the future, including reviewing and altering our security policies and procedures. We have engaged forensic computer experts to investigate the incident and determine the extent of information exposure, and are working to protect system passwords at all times. We apologize for any inconvenience this may have caused.

We value the security of your personal information and are therefore offering identity theft protection services through TransUnion 1B Credit Monitoring/Id Theft Restoration. This service includes twelve (12) months of credit monitoring, a \$1,000,000 insurance reimbursement policy, exclusive educational materials and fully managed identity theft recovery services. With this protection, TransUnion 1B Credit Monitoring/Id Theft Restoration will help you resolve issues if your identity is compromised.

WHAT YOU CAN DO

We have arranged for you to enroll, at no cost to you, in a twelve (12) month online credit monitoring service/ID Theft Restoration (*myTrueIdentity*) provided by TransUnion Interactive, a subsidiary of Transunion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code" enter the following 12-letter Activation Code <<Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

You can sign up for the online credit monitoring service anytime between now and [REDACTED]. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

If you believe you may be a victim of identity theft, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following [REDACTED] telephone pass code [REDACTED] to speak to a TransUnion representative about your identity theft issue.

For More Information

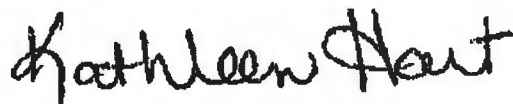
You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the following enrollment code below when calling or enrolling on the website, so please do not discard this letter.

Your Enrollment Code: [REDACTED]

Please call 877-347-0276 for assistance or for any additional questions you may have.

To reiterate, we have taken steps to prevent this from happening in the future, including reviewing our information security policies and procedures. We apologize for any inconvenience this may have caused.

Sincerely,



Kathleen Hart
Chief Information Officer
EnergyUnited EMC

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The contact information for all three credit bureaus is below:

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a freeze. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.