



## APPLIED ECOLOGICAL SERVICES

*SPECIALISTS IN ECOLOGICAL SCIENCE, RESTORATION, MANAGEMENT, AND RESEARCH*

17921 W SMITH ROAD • PO BOX 256 • BRODHEAD, WI 53520 • (608) 897-8641

July 12<sup>th</sup>, 2019

NAME  
ADDRESS  
CITY, STATE ZIP

Re: Data Security Incident

Dear \_\_\_\_\_:

This letter is to inform you that on June 17, 2019 Applied Ecological Services, Inc. ("AES") was subject to a ransomware attack. Some of AES' servers containing personal information of 497, in total, current and former employees and vendors were affected in this incident. The ransomware hackers obtained control of the servers, preventing AES from accessing them. The hackers threatened to destroy all of the information on the servers unless AES paid a specified sum. AES promptly consulted with IT security specialists who advised AES to pay the hackers. AES paid the ransom on June 18, 2019, and then regained full control of the server that same day.

AES promptly reviewed the information on the servers subject to the attack to determine what types of personal information were compromised, and who the affected individuals are. You are receiving this letter because some of your personal information was on the servers subject to the attack. The following categories of information were on such servers: name, address, driver's license number, dates of birth, and social security numbers.

AES is working with a cybersecurity firm to review its data security and to minimize the potential for future attacks. This firm is auditing AES' current IT security to determine ways in which it can be improved. AES will continue to work with this firm to implement its suggestions for improvement. AES is working with law enforcement to look into this incident as well, however, please note that this notice has not been delayed due to investigation.

It is important that you continue to review your financial account information and monitor your credit report to detect and address problems quickly. You should consider placing 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 account. The initial fraud alert stays on your credit report for one year, but you may renew it after one year. You may also want to consider placing a credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report, making it less likely that an identity thief can open new accounts in your name. If you wish to place fraud alert you must contact one of the following credit reporting agencies, and that agency will inform the other two. However, if you wish to place a security freeze on your credit you must contact all three major credit reporting agencies. Their contact information is:

Equifax  
www.equifax.com  
Fraud Alert:  
P.O. Box 105069  
Atlanta, GA 30348-5069  
800-525-6285  
Credit Freeze:  
P.O. Box 105788  
Atlanta, GA 30348-5788  
1-888-298-0045

Experian  
www.experian.com  
P.O. Box 9701  
Allen, TX 75013  
1-888-397-3742  
Credit Freeze:  
Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

TransUnion  
www.transunion.com  
Fraud Alert:  
P.O. Box 2000  
Chester, PA 19016  
800-680-7289  
Credit Freeze:  
P.O. Box 160  
Woodlyn, PA 19094  
888-909-8872

You can obtain further information about preventing identity theft from the Federal Trade Commission (“FTC”):

Federal Trade Commission  
600 Pennsylvania Ave, NW  
Washington, D.C. 20580  
877-382-4357  
www.ftc.gov

If you suspect your identity has been stolen, you should contact law enforcement, the Federal Trade Commission, and your state’s Office of the Attorney General.

If you would like to contact AES regarding this data security incident, please call 1-855-285-5373 or email [it.incidentresponse@appliedeco.com](mailto:it.incidentresponse@appliedeco.com). We apologize for the inconvenience that this incident causes you and are working diligently to increase our data security to prevent future incidents.