Template Correspondence to Individuals whose PII may have been accessed and/or exfiltrated:

**Subject: AAA Energy Services Co., Notice of Data Breach, Protective Measures Against Identity/Credit Theft**

**Notice of Breach Incident:**

On February 28, 2023, we experienced an unauthorized system lockdown to our computer system. We engaged computer forensic services and have determined that personally identifiable information (PII) from our files and other information from our computer system were accessed and copied or otherwise stolen as a result of unauthorized access to our system. Certain of such materials are now available on so called “dark web” sites.

We understand that the PII involved may include social security numbers, and potentially other PII among other information resident on our system.

As a result of the forensic investigation, we were advised that the system lock out resulted from the installation of ransomware known as Royal Ransomware.

Since the compromise of our system could have included these or other files where PII may be, you should consider whether other information relating to you and provided to AAA Energy Services could have included additional PII whose compromise must be considered or addressed.

We have not paid a ransom to the criminals responsible for this attack on our computer system, but we have notified federal authorities and are notifying state attorneys general in New Hampshire and in Maine, in addition to the FBI. We have also implemented additional security measures in connection with our computer system and will be considering additional measures and policies to strengthen our system and reduce this risk which faces AAA Energy Services and everyone who uses computer systems and the internet.

**What You Can Do To Minimize Your Risks And Impacts Of Identity Theft**

The principal risks from stolen PII include unauthorized credit risks and risks to governmental transactions including tax returns and government benefits. Attached to this email is a pdf from the Social Security Administration reflecting governmental resources available when social security numbers have been stolen and/or used.

With respect to risks involving tax filings and refunds we urge you to review information from the IRS (<https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft>).

With respect to risks regarding Social Security, we enclose a copy of a pamphlet from the Social Security Administration entitled "Identity Theft And Your Social Security Number.”

With respect to unauthorized credit risks, it is recommended that you immediately lock down your credit reports with each of the credit rating agencies (E.g.Ch Transunion, Experian, etc.) if you have not already done so. When locked, no third parties are allowed to make credit inquiries or open credit accounts in your name even if they have your social security number, unless and until you unlock your account for that purpose. Further information on this process is available here: <https://www.nerdwallet.com/article/finance/how-to-freeze-credit>

While some commentators believe that third party credit and/or identity theft monitoring is unnecessary if your credit reports are locked, we leave that decision to you and are willing to reimburse the reasonable costs of such monitoring for a period of 3 months for any employee, with copies of the monitoring reporting from the service. For example, we note that Equifax Complete provides such services for 19.95 per month. Other similar reasonable cost services may be used with our prior consent.

Please contact me if you have any questions, or if you receive any information that your personally identifiable information may have been used without your permission.

Regards,

Chad Everett

Service Manager

AAA Energy Service Co.

(207) 883-1473