WHITEFORD, TAYLOR & PRESTON L.L.P.

SPENCER S. POLLOCK
DIRECT LINE (410) 832-2002
DIRECT FAX (410) 339-4028
spollock@wtplaw.com

7 ST. PAUL STREET
BALTIMORE, MD 21202-1636
MAIN TELEPHONE (410) 832-2000
FACSIMILE (410) 832-2015

DELAWARE*
DISTRICT OF COLUMBIA
KENTUCKY
MARYLAND
NEW YORK
PENNSYLVANIA
VIRGINIA

WWW.WTPLAW.COM
(800) 987-8705

February 20, 2022

Privileged and Confidential
SUBMITTED VIA THE ONLINE PORTAL ONLY:
https://appengine.egov.com/apps/me/maine/ag/reportingform
Office of the Attorney General

Re: Security Breach Notification

Dear Sir or Madam,

We are writing on behalf of our client JMA Energy ("JMA") (located at 1021 NW Grand Boulevard, Oklahoma City, OK 73118), to notify you of a data security incident involving ten (10) Maine residents.[1]

Nature

On December 6, 2021, JMA discovered that they were the victim of a sophisticated ransomware attack that resulted in encryption and unauthorized access to their network. At that time, JMA took immediate steps to stop the threat and understand the full scope of the situation. This included hiring third-party forensic experts to conduct a thorough investigation and assist in the remediation efforts. On January 14, 2022, JMA concluded its initial investigation and found that the unauthorized individual gained access to its systems via a malicious software that remained hidden but has since been remediated.

At that time, JMA began a comprehensive search of the data to determine what information was involved and the individuals the incident impacted. JMA recently concluded its review and determined that the incident involved personal information related to Maine residents. ***However, as of now, there is no evidence indicating identity theft or financial harm involving any of the information.*** On February 17, 2022, JMA confirmed the most recent contact information of these individuals.

This information may have included, but not be limited to, names, addresses, phone numbers, social security numbers, tax ID numbers, banking and other financial information (but to our knowledge, not security access information related to banking information).

Notice and JMA's Response to the Event

[1] By providing this notice, JMA does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine's data event notification statute, or personal jurisdiction.

On February 23, 2022, JMA will mail a written notification to the potentially affected Vermont residents, pursuant to pursuant to pursuant to 9 V.S.A § 2435, in a substantially similar form as the enclosed letter (attached as Exhibit A).

Additionally, JMA is providing these potentially impacted individuals the following:

- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank.
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- A reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports; and
- Encouragement to contact the Federal Trade Commission and law enforcement to report attempted or actual identity theft and fraud.

Further, JMA provided the notice to the three national credit reporting agencies along with the applicable government regulators, officials, and other Attorneys General (as necessary).

Finally, JMA is working to implement any necessary additional safeguards, enhance and improve its policies and procedures related to data protection, improve its cybersecurity infrastructure, and further train its employees on best practices to minimize the likelihood of this type of incident occurring again.

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 832-8002 or email me at spollock@wtplaw.com.

Sincerely Yours,

Spencer S. Pollock, Esq., CIPP/US, CIPM

EXHIBIT A

JMA Energy
P.O. Box 3923
Syracuse, NY 13220

JMA
ENERGY COMPANY
1021 NW Grand Boulevard
Oklahoma City, OK 73118

[redacted]

February 23, 2022

NOTICE OF SECURITY INCIDENT

We are writing to let you know about a data security incident that may have involved personal and/or business information that you have provided to JMA Energy Company, LLC ("JMA") and/or one of its affiliated entities in connection with your business dealings with those entities. In sum, our internal computer systems were the subject of a ransomware attack. Importantly, we are currently unaware of any actual misuse of your information due to this attack. Nevertheless, we are reaching out to you to provide you with information so that you may take all measures you deem necessary to protect against possible identity theft, fraud, and other unlawful or unauthorized conduct.

What Happened and What Information Was Involved.
On December 6, 2021, we discovered that we were the victim of a sophisticated cyber incident attack. After discovering the incident, we quickly secured our systems and operations. Further, we immediately engaged independent third-party forensic and incident response experts to thoroughly investigate the incident's nature and scope and assist in remediation efforts. Our investigation is ongoing, but we recently learned that the incident involved some information in our systems.

As a result of this attack, information about individuals and/or business entities may have been accessed, copied, or otherwise used by the attacker without our consent. This information may have included, but not be limited to, names, addresses, phone numbers, social security numbers, tax ID numbers, banking and other financial information, and confidential documents and agreements we have in our possession. Accordingly, we are notifying you about this security incident. We do not believe the incident involved the password or other credentialing information associated with any of your personal or business email accounts.

What We Are Doing.
Since the attack, our information security personnel have investigated the matter to endeavor to ensure that the intrusion was isolated and prevent additional information from being accessed. We are also actively monitoring our network to safeguard it from further attack. As stated above, we have also engaged an outside forensic cybersecurity firm to ensure that the malware at issue has been removed from our systems and our internal information is no longer subject to attack, as well as to provide an analysis, to the extent possible, of whether the information accessed has been misused. As a result of these efforts, we believe the attack has been contained and prevented from further access into our computer network; however, we would encourage you to remain diligent in monitoring for any suspicious activity concerning your information.

What You Can Do.
Although we are unaware of any actual misuse of your information, we want to make you aware of certain steps you may take to guard against identity theft or fraud which are found on the reverse side of this letter entitled "Steps You Can Take to Protect Your Information".

For More Information.

We understand that you may have questions about it beyond what is covered in this letter. If you have additional questions, please call our toll-free response line at [redacted], Monday through Friday between 8:00 a.m. and 8:00 p.m. (ET), except holidays. Representatives are available for 90 days from the date of this letter. Please provide the following code when calling: [redacted]

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

Review your financial account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint with the FTC, go to *IdentityTheft.gov* or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Obtain and Monitor Your Credit Report

You should obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting *http://www.annualcreditreport.com*, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at *https://www.annualcreditreport.com/requestReport/requestForm.action*. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

- **Equifax**, (866) 349-5191, *www.equifax.com*, P.O. Box 740241, Atlanta, GA 30374
- **Experian**, (888) 397-3742, *www.experian.com*, P.O. Box 2002, Allen, TX 75013
- **TransUnion**, (800) 888-4213, *www.transunion.com*, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016

Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Take Advantage of Additional Free Resources on Identity Theft

Review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security. For more information, please visit *IdentityTheft.gov* or call 1-877-ID-THEFT (877-438-4338).

Security Freeze

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may contact one of the three credit reporting agencies identified above. You may be required to provide information that identifies you including your full name, social security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. Depending on where you live, there should be no charge to request a security freeze or to remove a security freeze.

Iowa residents may also wish to contact the Office of the Attorney general on how to avoid identity theft by calling 515-281-5164 or by mailing a letter to the Attorney General at: *Office of the Attorney General of Iowa,* Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319. **Maryland residents** may wish to review the information the Attorney General, who can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, or visiting www.oag.state.md.us. **New Hampshire residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above. **New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit. **New York Residents**: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: *New York Attorney General's Office Bureau of Internet and Technology*, (212) 416-8433, https://ag.ny.gov/internet/resource-center and or NYS Department of State's Division of Consumer Protection, (800) 697-1220, https://www.dos.ny.gov/consumerprotection. **North Carolina residents** may wish to review the information provided by the North Carolina Attorney General at www.ncdoj.gov, or by contacting the Attorney General by calling 877-5-NO-SCAM (Toll-free within North Carolina) or by mailing a letter to the Attorney General at *North Carolina Attorney General's Office, Consumer Protection Division,* 9001 Mail Service Center Raleigh, NC 27699. **Oregon Residents**: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877- 9392, www.doj.state.or.us. **Rhode Island residents** have the right to obtain a police report (if one was filed. Alternatively, you can file a police report). Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. **West Virginia residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above.