

**VIA E-MAIL**

Consumer Protection Bureau  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301  
DOJ-CPB@doj.nh.gov

**Re: Notice of Security Incident**

Dear Attorney General MacDonald:

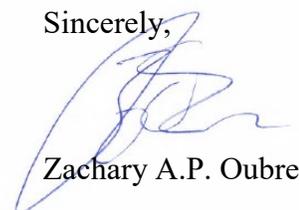
On behalf of JMA Energy Company, LLC (“JMA Energy”), we are notifying your office of a data security incident potentially involving the information of five (5) New Hampshire residents.

On or about December 15, 2020, JMA Energy learned that malware had been placed on its servers denying access to its computer system and data. As a result of this attack, information about individuals that have done business with JMA may have been accessed, copied or otherwise used by the attacker without JMA Energy's consent. This information may have included, but not be limited to, names, addresses, phone numbers, social security numbers, and banking information (but to our knowledge, not security access information related to banking information). Consumer notification letters were sent out on or about January 22, 2021. A template copy of that notification letter is enclosed.

Since the attack, JMA Energy's information security personnel have investigated the matter to endeavor to ensure that the intrusion was isolated and prevent additional information from being accessed. JMA Energy is also actively monitoring its network to safeguard it from further attack. JMA Energy has also engaged an outside forensic cybersecurity firm to ensure that the malware at issue has been removed from its systems and its 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, JMA Energy believes the attack has been contained and prevented from further access into its computer network.

We had previously notified your office of the incident on or about January 29, 2021 and were asked for additional information on or about February 1, 2021. If you have any questions, or require further information, please let me know.

Sincerely,



Zachary A.P. Oubre



[Date of Notice]

[Customer's Name]

[Address Line 1]

[Address Line 2]

[City, State] [Zip]

## **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 as a result of this attack. Nevertheless, we are reaching out to you to provide you 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 or about December 15, 2020, we learned that malware had been placed on our servers denying us access to our computer system and data. 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. 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”. You may use the contact information set forth therein to contact credit reporting and other agencies about fraud alerts, security freezes and other ways to protect against identity theft and other misuse of your personal information.

### **For More Information.**

If you have further concerns about this incident, or need any further assistance, please contact us at the following email address, [data.inquiries@jmaenergy.com](mailto:data.inquiries@jmaenergy.com), or contact us by phone at 1-866-718-2081. We will endeavor to respond to your inquiries in a timely fashion. We sincerely regret any inconvenience or concern caused by this incident.

## **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](http://www.equifax.com), P.O. Box 740241, Atlanta, GA 30374
- **Experian**, (888) 397-3742, [www.experian.com](http://www.experian.com), P.O. Box 2002, Allen, TX 75013
- **TransUnion**, (800) 888-4213, [www.transunion.com](http://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.