LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

March 1, 2024

Via electronic-mail: *DOJ-CPB@doj.nh.gov*; *AttorneyGeneral@doj.nh.gov*

Attorney General John M. Formella
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re:	**Our Client**	**:**	**Muscatine Power and Water**
	Matter	**:**	**January 2024 Data Security Incident**
	LBBS File No.	**:**	**16516.381**

Dear Attorney General Formella:

We represent Muscatine Power and Water ("MPW") principally located in Muscatine, Iowa with respect to a data security incident described in more detail below. MPW takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the incident, the number of New Hampshire residents being notified, what information has been compromised, and the steps that MPW is taking to restore the integrity of its information system. We have also enclosed hereto a sample of the notification to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On January 26, 2024, MPW discovered that it was the target of a cybersecurity incident that may have resulted in the exposure of personal information. Although we have found no evidence that any information has been specifically accessed for misuse, it is possible that the potentially impacted individuals'

could have been exposed as a result of this incident.

As of this writing, MPW has not received any reports of related identity theft since the date the incident was discovered (January 26, 2024 to present).

2. Number of New Hampshire Residents Affected

A total of three (3) residents of New Hampshire were potentially affected by this security incident. A notification letter to these individuals are scheduled to be mailed on March 1, 2024 by first class mail including an offer of free credit monitoring. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Upon learning of this incident, MPW moved quickly to initiate a response plan, which included conducting an investigation with the assistance of third-party forensic specialists. Since then, MPW has been working with law enforcement to help respond to the incident, along with cybersecurity experts to review all policies and procedures relating to the security of MPW's systems.

Although MPW is not aware of any evidence of misuse of personal information, MPW extended to all potentially impacted individuals an offer for free credit monitoring and identity theft protection through Cyberscout. This service will include of credit monitoring, along with fully managed identity theft recover service, should the need arise.

4. Contact Information

MPW remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at .

Very truly yours,

Robert F. Walker of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Copy: Nicholas Chauvin, Esq. (Lewis Brisbois LLP)

Enclosure: *Sample Notification Letter*

Muscatine Power and Water
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

P
[redacted]

March 1, 2024

0000101102G0500

P

Via First-Class Mail

Notice of Potential Data Security Incident

Dear [redacted],

You are receiving this letter because you are a current or former customer of Muscatine Power and Water ("MPW"). We are writing to inform you of an incident that may have exposed your personal information. MPW takes your privacy and security seriously. As such, this letter contains details about the incident and resources to help protect your personal information going forward.

What Happened:

On or about January 26, 2024, MPW was the target of a cybersecurity incident that involved an unauthorized party gaining brief access to our corporate network environment. Upon detecting the incident, we immediately conducted an internal investigation and engaged a specialized third-party forensic incident response firm to assist with securing the network environment and determining the scope and extent of unauthorized activity. Our network environment has been secured and there is no evidence of any ongoing malicious activity.

What Information Was Involved:

After the comprehensive forensic investigation into this incident concluded, we discovered that your

may have been exposed in the attack. We have had no reports of related identity theft as a result of this incident.

What We Are Doing:

The security and privacy of personal data remains one of MPW's highest priorities. We have engaged external cybersecurity experts and are taking steps to prevent a similar event from occurring in the future by implementing additional safeguards and enhanced security measures to better protect the privacy and security of information in our systems. We have also reviewed and taken steps to enhance our policies and procedures relating to the security of our systems, as well as our information life cycle management.

Additionally, in response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. We are also providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/muscatinepw** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information:

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-833-961-6762 and be prepared to supply the fraud specialist with your unique code listed within. MPW's customer service and HelpDesk staff, unfortunately, are not able to support you with setting up credit monitoring. Please call TransUnion directly.

We encourage you to take full advantage of these services. Enclosed you will find additional materials regarding the resources available to you, and the steps you can take to further protect your personal information.

Again, we value the security of the personal data that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused. We appreciate your patience and consideration.

Muscatine Power and Water Team

Additional Information

Credit Reports: 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.

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, 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 security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/	**Experian Security Freeze** P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	**TransUnion Security Freeze** P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (https://www.transunion.com/fraud-alerts); or
- Experian (https://www.experian.com/fraud/center.html).

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 phone numbers for all three credit bureaus are listed above.

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

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For 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 reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.
For New York residents, the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and https://ag.ny.gov/.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 2 Rhode Island residents that may be impacted by this event.