LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

October 3, 2019

File No. 32587.35

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

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent The Board of Public Works for The City of Lewes ("Lewes BPW"), a locally owned and operated utility that regulates electric, water, and sewer systems for the City of Lewes in Delaware. This letter is being sent pursuant to N.H. Rev. Stat. §§ 359-C:19 - C:21, because the personal information of two (2) New Hampshire residents may have been affected by a recent data security incident. The incident may have included unauthorized access to names, active and inactive credit card numbers with expiration dates (without security codes), and/or financial account numbers.

On May 28, 2019, Lewes BPW was notified by local police and the U.S. Secret Service that payment card information belonging to Lewes BPW customers had been identified on the dark web. Lewes BPW immediately secured its system and launched an investigation with the assistance of an independent digital forensics firm to help determine what occurred and whether sensitive information was accessed or acquired without authorization as a result. On August 6, 2019, the forensics firm reported that an unauthorized actor had acquired payment information stored on a Lewes BPW database for customers making recurring payments. On August 18, 2019, Lewes BPW confirmed that two (2) New Hampshire residents were included within the potentially affected population.

Lewes BPW is not aware of any unauthorized financial transactions as a result of this incident. Additionally, credit card security codes were not stored in the database. Lewes BPW has notified the major payment card brands (American Express, Discover, MasterCard, and Visa) about the incident, and is cooperating with the FBI and U.S. Secret Service to support the ongoing investigation.

Lewes BPW notified the affected New Hampshire residents via the attached sample letter on October 2 and 3, 2019. Lewes BPW previously offered twelve (12) months of complimentary credit monitoring services through LifeLock to residents whose active credit cards or financial account numbers were potentially impacted. In response to the incident, Lewes BPW has implemented numerous enhanced security features, and continues to work internally and with external cybersecurity resources to help prevent a similar incident from occurring in the future.

Please contact me should you have any questions.

Sincerely,

/s/ Alyssa R. Watzman

Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Consumer Notification Letter

Lewes BPW
Electric, Water, and Sewer Utility

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notification of Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing at this time to provide an update about a data security incident involving suspected unauthorized access to a database containing your name and credit card or bank account information. The Board of Public Works of the City of Lewes ("Lewes BPW") takes the privacy and security of all personal information very seriously. That is why I am writing to provide you with additional information about this incident and about steps that you can take to help protect your personal information.

What Happened? On May 28, 2019, Lewes BPW learned that payment data stored within a Lewes BPW database had been accessed / acquired without authorization. Upon discovering this information, Lewes BPW immediately took steps to secure the data and launched an investigation. On May 29, 2019, I sent you an initial letter relating to this incident. Lewes BPW then engaged a leading, independent forensics firm to determine what happened and whether sensitive information was accessed or acquired without authorization as a result. On August 6, 2019, that firm reported that an unauthorized actor acquired payment information stored within a Lewes BPW database for customers making recurring payments.

Lewes BPW is not aware of any misuse of information potentially impacted in connection with this incident, including unauthorized financial transactions having occurred as a result of this incident. I am writing to provide additional information about this incident out of an abundance of caution.

What Information Was Involved? The information involved may have included your name and credit card number along with the relevant expiration date (without security codes), or bank account information.

What Are We Doing? As soon as Lewes BPW discovered this incident, Lewes BPW took the measures referenced above. With the assistance of independent cybersecurity experts, Lewes BPW also implemented enhanced security measures in order to better safeguard all personal information and to help prevent a similar incident from occurring in the future. In addition, Lewes BPW is cooperating with law enforcement to help hold the perpetrators of this incident accountable and is providing you with the enclosed information about steps you can take to help protect your personal information.

What You Can Do. Lewes BPW recommends that you review the guidance on the next page about how to help protect your personal information.

For More Information. If you have questions or need assistance, please contact 1-???-???-???? Monday through Friday, 8:00 a..m. to 5:30 p.m., Central Time. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Darrin Gordon
General Manager
The Board of Public Works of The City of Lewes

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your 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, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may 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 print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Fraud Alert: 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 one (1) year. 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.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf