RECEIVED
MAR 14 2022
CONSUMER PROTECTION

MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

March 11, 2022

**VIA U.S. MAIL**

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent Bonita Springs Utilities, Inc. ("BSU") located at 11900 East Terry Street Bonita Springs, FL 34135, and are writing to notify your office of an incident that may affect the security of some personal information relating to twenty (20) New Hampshire residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, BSU does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

BSU uses IberiaBank to collect and process payments BSU receives from its customers. IberiaBank in turn utilizes a lockbox service provided by Technology Management Resources, Inc. ("TMR") for these payments.

On or about January 6, 2022, BSU received notice from IberiaBank of a data security event involving TMR's lockbox service. According to IberiaBank, TMR identified unusual activity with a user account in its client payment application on or around October 14, 2021. TMR investigated and determined an unauthorized actor may have had access to the payment application between October 12, 2021 and October 14, 2021. This application enabled access to certain information that could be used to convert images of customer documents uploaded to IberiaBank's lockbox. Importantly, IberiaBank's notice advised that the investigation was ongoing and it had not determined that BSU data had been impacted by the lockbox incident.

Upon learning of the incident, BSU promptly responded and requested additional information from TMR and IberiaBank to identify any risk to BSU customer information. On February 10, 2022, IberiaBank provided additional information and BSU determined personal information as defined by N.H. Rev. Stat.

Ann. § 359-C:19 could have been accessed as a result of the lockbox incident. The personal information involved includes name and financial account information.

**Notice to New Hampshire Residents**

On or about March 11, 2022, BSU began providing written notice of this incident to twenty (20) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

**Other Steps Taken and To Be Taken**

As stated above, upon discovering the event, BSU moved quickly to investigate and respond, including working with both TMR and IberiaBank to confirm the nature and scope of the incident so it could assess any risk to BSU customer information. BSU is considering appropriate additional measures as result of this incident, including reviewing and procedures with vendors.

While BSU is unaware of any misuse of BSU customer information, it arranged for its potentially affected customers to receive access to twelve (12) months of complimentary credit monitoring services. Additionally, BSU is providing individuals with guidance on how to better protect against identity theft and fraud. BSU is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, 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, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

**Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,

Sian M Schafle.

Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/aml
Enclosure

# EXHIBIT A

[First Name] [Last Name]
[Address]
[City, State, Zip]

[Date]

**Re: Notice of [Variable1]**

Dear [Name],

Bonita Springs Utilities, Inc. ("BSU") is writing to notify you that you may have been affected by a Technology Management Resources, Inc. ("TMR") data security event. TMR is a third-party lockbox service provider utilized by IberiaBank. BSU uses IberiaBank to collect and process payments from our customers. To date, neither TMR nor IberiaBank have reported that your information has been misused as a result of TMR's incident. Although this event did not affect BSU systems, we wanted to provide you with information on the event and the resources available to you to help protect your information, should you feel it appropriate to do so.

**What Happened?** On or about January 6, 2022, IberiaBank disclosed the TMR data security event to BSU. IberiaBank's notice reported that on October 14, 2021, TMR identified unusual activity with a user account in its client payment application. TMR determined that that the activity was unauthorized and occurred between October 12, 2021 and October 14, 2021, and during that time the unauthorized actor may have had access to certain information including images of customer documents uploaded to IberiaBank's lockbox. On February 10, 2022 IberiaBank informed BSU that the security incident affected BSU customers and provided a list of those customers.

**What Information Was Involved?** IberiaBank reported that the information present in the involved lockbox account includes your name and [date element].

**What We Are Doing.** We take the confidentiality, privacy, and security of personal information very seriously. After receiving notice from IberiaBank, we took steps to understand the impact the TMR event had on BSU data. As part of our ongoing commitment to the security of our members, we are working to evaluate additional measures and safeguards in response to this incident. As an added precaution, we arranged to have TransUnion provide credit monitoring services for 12 months at no cost to you.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity. You may review the information contained in the enclosed "*Steps You Can Take to Help Protect Personal Information*." You may also enroll in the complimentary identity credit monitoring services we are making available to you. Enrollment instructions are attached to this letter.

**For More Information.** We understand you may have questions about the TMR event that are not addressed in this letter. If you have questions, please call BSU at (239) 992-0711 Monday through Friday 7:30 am – 5:00 pm (excluding major U.S. holidays). You may also contact BSU by email at customerservice@bsu.us or by mail at 11900 East Terry Street, Bonita Springs, FL 34135.

Sincerely,

Customer Service Manager

## STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

**Enroll in Credit Monitoring**

TransUnion

**Activation Code: <<Activation Code>>**

**1-Bureau TransUnion Credit Monitoring Product Offering:** (Online and Offline)

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for 12 months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the myTrueIdentity website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass coc and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain 12 months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the myTrueIdentity online Credit Monitoring service anytime between now and June 30, 2022. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your myTrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the myTrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

**Monitor Your Accounts**

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| https://www.equifax.com/personal/credit-report-services/ | https://www.experian.com/help/ | https://www.transunion.com/credit-help |
| 888-298-0045 | 1-888-397-3742 | 833-395-6938 |
| Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069 | Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013 | TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016 |
| Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788 | Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013 | TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094 |

**Additional Information**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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 and your state Attorney General. This notice has not been delayed by law enforcement.

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. BSU is located at 11900 East Terry Street, Bonita Springs, FL 34135.

*For New York residents*, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

*For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 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 20 Rhode Island residents impacted by this incident.