clarity
water technologies llc

87 Hunt Rd., Orangeburg, NY 10962 • Ph: 888-616-3545 • Fax: 888-754-4304 • E-Mail: accounting@claritywatertech.com

February 24, 2023

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

RE: Notification of Data Breach

Dear Office of the New Hampshire Attorney General Representative:

Pursuant to N.H. Rev. Stat. Ann. § 359-C:20, we are notifying the Office of the New Hampshire Attorney General of a data breach, affecting approximately 4 New Hampshire residents. Clarity Water Technologies ("Clarity") is a New York-based small business with approximately employees.

On the morning of Sunday, February 12, 2023, we discovered that a cyber-criminal had launched an attack on our computer network. We discovered the attack at approximately 8am that morning and Citadel Blue, our information systems support company, immediately began to investigate and protect our computer system.

Citadel Blue informed us that the attack had begun a few hours earlier (at approximately 4am that morning) and affected 5 computer desktops. Citadel Blue moved swiftly to block the cyber-criminal's access to our systems, repair the affected computers, and ensure that the cyber-criminal had no further access to our company or its computer system.

Due to our comprehensive back-up systems and Citadel Blue's rapid response to the attack, Clarity was fully operational at all times and did not lose any files, records, or other information. There has not been, and continues to be, no impact on Clarity's operations or its ability to serve its customers.

Nevertheless, Citadel Blue could not rule out that the cyber-criminal may have obtained access to copies of information Clarity holds about its workforce members, including current or former employees or dependents of a current or former employee. This information may have included: (a) Social Security number; (b) name, address, and contact information; (c) benefit information; and (d) personnel file information.

We have no evidence that the cyber-criminal in fact accessed the personal information of workforce members, acquired any copies of it, or misused it in any way. In fact, Citadel Blue's continuing investigation indicates that the cyber-criminal may have acted through an "automated procedure" and had no special interest in Clarity (this cyber-criminal is known to attack financial firms, such as banks).

Clarity is providing written notice to all individuals identified as having information potentially affected by this incident. Included with this notice is a "Reference Guide" which provides useful information regarding steps individuals may take to protect their identity, including obtaining copies of a credit report and implementing credit freezes. In addition, Clarity is offering our employees 24 months of identity theft protection services.

I want to assure you that Clarity takes its obligation to protect the privacy and confidentiality of its workforce's personal information very seriously, and while no business is 100% secure in this day and age, Clarity is working with Citadel Blue to evaluate ways in which we can reduce the likelihood of a future cyber-attack. If you have any questions, please contact me at 845-640-5013.

Sincerely,

87 Hunt Road • Orangeburg, NY 10962 • Ph: 888-616-3545 • E-Mail: accounting@claritywatertech.com

February 24, 2023

Dear Clarity Current or Former Associate:

We recently discovered that Clarity Water Technologies was the victim of a criminal cyber incident that may have involved some of the personal information we hold about you. We are writing to provide information to you about it.

On the morning of Sunday, February 12, 2023, Clarity discovered that a cyber-criminal had launched an attack on Clarity's computer network. Clarity discovered the attack at approximately 8am that morning and Clarity's information systems support company immediately began to investigate and protect Clarity's computer system. They then moved swiftly to block the cyber-criminal's access to Clarity, repair the affected computers, and ensure that the cyber-criminal had no further access to Clarity or its computer system. Clarity was fully operational at all times and did not lose any files, records, or other information. There has not been, and continues to be, no impact on Clarity's operations or its ability to serve its customers.

Nevertheless, our information systems support company informed us that we cannot rule out that the cyber-criminal may have obtained access to copies of information we hold about you, such as through your role as a current or former employee or dependent of a current or former employee. The total number of individuals whose information may have been accessed was 154. This information may have included the following about you: (a) bank account information, such as for direct deposit; (b) Social Security number; (c) name, address, and contact information; (d) benefit information (such as name of health plan or insurance carrier); and (e) personnel file information (such as salary and bonus information).

Please note that we have no evidence that the cyber-criminal in fact accessed your information, acquired any copies of it, or has misused it in any way. In fact, our information systems support company's continuing investigation indicates that the cyber-criminal may have acted through an "automated procedure" and had no special interest in Clarity (this cyber-criminal is known to attack financial firms, such as banks).

1. Protecting Your Information

We are providing written notice to all individuals that we have identified as having information potentially affected by this incident. Included with this notice is a "Reference Guide" which provides useful information regarding how to protect your identity, including obtaining copies of your credit report and implementing credit freezes. We encourage you to review the Reference Guide closely.

87 Hunt Road • Orangeburg, NY 10962 • Ph: 888-616-3545 • E-Mail: accounting@claritywatertech.com

2. Our Response

Clarity is notifying relevant state and federal authorities of this cyber-attack. While no business is 100% secure in this day and age, we are working with our information systems support company to evaluate ways in which we can reduce the likelihood of a future cyber-attack.

3. For More Information

Clarity takes its obligation to protect the privacy and confidentiality of our workforce's personal information very seriously. We sincerely regret that this occurred. If you have any questions, you may contact us by phone at .

Sincerely,

Pete Stempkowski & Tom Hageman
Co-Managing Partners
Clarity Water Technologies, LLC

87 Hunt Road • Orangeburg, NY 10962 • Ph: 888-616-3545 • E-Mail: accounting@claritywatertech.com

Reference Guide

Review Your Account Statements. We encourage you to remain vigilant by reviewing your account statements. If you believe there is an unauthorized charge on your card, please contact your financial institution or card issuer immediately. The payment card brands' policies provide that cardholders have zero liability for unauthorized charges that are reported in a timely manner. Please contact your card brand or issuing bank for more information about the policy that applies to you.

Order A Free Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580

1-877-ID-THEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 2002 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. For more information on security freezes, you may contact the three nationwide consumer reporting agencies, or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

87 Hunt Road • Orangeburg, NY 10962 • Ph: 888-616-3545 • E-Mail: accounting@claritywatertech.com

Equifax	Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	1-800-349-9960	www.equifax.com/personal/credit-report-services/
Experian	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com/freeze/center.html
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-888-909-8872	www.transunion.com/credit-freeze

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)
- Social Security Card, pay stub, or W2
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Additional Information for North Carolina Residents. You can also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (Toll-free within North Carolina)
919-716-6000
www.ncdoj.gov

Additional Information for Rhode Island Residents. Under Rhode Island law, you have the right to file and obtain a police report regarding this incident and obtain a copy of it. You can contact the Rhode Island Attorney General to learn more about how to protect yourself from becoming a victim of identity theft:

87 Hunt Road • Orangeburg, NY 10962 • Ph: 888-616-3545 • E-Mail: accounting@claritywatertech.com

Office of the Rhode Island Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401) 274-4400
consumers@riag.ri.gov
http://www.riag.ri.gov

Additional Information for Maryland Residents: You may obtain information from these sources on steps you can take to prevent identity theft.

Office of the Maryland Attorney General
200 St. Paul Place, 25th Floor, Baltimore, MD 21202
(410) 576-6491
Fax: (410) 576-6566
idtheft@oag.state.md.us

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580

1-877-ID-THEFT (438-4338)
www.ftc.gov/idtheft/