June 28, 2013

Attorney General Joseph Foster
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Dear Attorney General Foster:

Pursuant to New Hampshire Rev. Stat. Ann. § 359-C:20(I)(b), this letter is to inform you of a data security incident that occurred on or around April 11, 2013. The incident was discovered approximately one day later and an investigation was immediately initiated.

Bridgewater offers employees continuing health care coverage (COBRA) upon their separation from Bridgewater. Bridgewater utilizes a third party provider (Ceridian) to administer these benefits. Ceridian hosts a database containing certain personal information for those former employees and dependents who are eligible to receive or who elect to receive continuing benefits. This personal information included employees' names, dates of birth, Social Security numbers, addresses, dates of separation from Bridgewater, type of separation, benefit plans elected while employed by Bridgewater, premiums and due dates, the length of time that individuals are eligible for continuing COBRA coverage and the same information for any dependents. **The database did not include any personal health information or any specifics of medical care or benefits that former employees or their family members may have received.** At this time we believe that approximately 11 New Hampshire residents were affected. They are being notified by mail simultaneously with our notification to you, and a copy of that notice is attached hereto.

The data security incident came to our attention when we learned that the password used by a Bridgewater consultant to access the database had been changed without the user's authorization. Upon investigating, it was confirmed that on three separate occasions, the Bridgewater consultant's unauthorized credentials were used to access a database containing the personal information. The identity of the unauthorized user is unknown at this time as is the information, if any, that may have been accessed. Bridgewater has no specific reason to conclude that any individual's personal information was accessed, but we are taking a conservative approach and because this information was contained in the database, we are providing individuals and the proper state authorities with this notice. This notification has not been delayed because of a law enforcement investigation.

Bridgewater takes very seriously our obligation to safeguard the personal information of current and former employees and to use it in an appropriate manner. We are in the process of finding a new vendor to maintain this database, and are also reviewing our contracts with all of our outside vendors. Although we have no reason to believe the password compromise was due to a failure on the part of our consultant to safeguard its confidentiality, we also are reinforcing to all employees and consultants with access to personal information the imperative – already set out in company policy – to select robust passwords and to keep log-in credentials confidential.

As a cautionary measure, we are offering credit monitoring services to affected individuals at no cost in order to protect against any misuse of information. We have arranged with Equifax Personal Solutions to help protect the identity and credit information of affected individuals for one year.

We will continue to assess our security measures to explore ways to protect and improve the security of the personal information we or our service providers maintain. Should you have any questions or

concerns regarding this matter, please contact us at One Glendinning Place Westport, CT 06880 or 203.226.3030 for additional information.

Sincerely,

Emily Kirsch – Head of Corporate Counsel and Corporate Secretary

June 28, 2013

**Activation Code:**

Dear,

This letter is to inform you of a data security incident that occurred on or around April 11, 2013. The incident was discovered approximately one day later and an investigation was immediately conducted.

As a former or rehired Bridgewater employee, you were offered continuing health care coverage (COBRA) upon your separation from Bridgewater. Bridgewater utilizes a third party provider (Ceridian) to administer these benefits. Ceridian hosts a database containing certain personal information for those former employees and dependents who are eligible to receive or who elect to receive continuing benefits. This personal information included your name, date of birth, Social Security number, address, date of separation from Bridgewater, type of separation, benefit plans elected while employed by Bridgewater, premiums and due dates, the length of time that you are eligible for continuing COBRA coverage and the same information for any dependents. **Please be aware that the database did not include any personal health information or any specifics of medical care or benefits that you or your family member may have received.**

The data security incident came to our attention when we learned that the password used by a Bridgewater consultant to access the database had been changed without the user's authorization. Upon investigating, it was confirmed that on three separate occasions, the Bridgewater consultant's unauthorized credentials were used to access a database containing your personal information. The identity of the unauthorized user is unknown at this time as is the information, if any, that may have been accessed. Bridgewater has no specific reason to conclude that your personal information was accessed, but we are taking a conservative approach and because your information was contained in the database, we are providing you with this notice.

As a cautionary measure, we would like to offer credit monitoring services to you at no cost in order to protect against any misuse of information. We have arranged with Equifax Personal Solutions to help you protect your identity and your credit information for one year. Please see the attached document to enroll in the service.

Bridgewater takes very seriously our obligation to safeguard your personal information and to use it in an appropriate manner. We will continue to assess our security measures to explore ways to protect and improve the security of the personal information we or our service providers maintain. Should you have any questions or concerns regarding this matter and/or the protections available to you, please contact us at Benefits_Help@bwater.com for additional information.

Sincerely,

Jen Vanderwall –Human Resources - Benefits

Stuart Friedman – Human Resources

As an additional precaution, it is recommended that you contact your bank and any credit card companies immediately to notify them of the potential disclosure of your Social Security number. Going forward, you should continue to monitor your account statements for evidence of fraud. Report any suspected incidents of identity theft to local law enforcement or your Attorney General. You also may take the following precautions to safeguard your personal information:

- Call the toll-free numbers of any one of the three major credit bureaus to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.

    - **Equifax**: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374

    - **Experian**: 1-888-397-3742; www.experian.com; Experian Fraud Division, P.O. Box 9530, Allen, TX 75013

    - **TransUnion**: 1-800-680-7289; www.transunion.com; TransUnion Fraud Victim Assistance Department, P.O. Box 6790, Fullerton, CA 92834

- Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.

- Call the Federal Trade Commission to get more information about fraud and identity theft. The FTC operates a call center for identity theft victims where counselors tell consumers how to protect themselves and what steps to take if they become victims of identity theft.

    - **Federal Trade Commission**: 1-877-IDTHEFT (1-877-438-4338); www.ftc.gov/idtheft; 600 Pennsylvania Avenue, NW, Washington, DC 20580

- Consider placing a security freeze on your credit reports. Unlike a fraud alert, which is free and alerts creditors to employ heightened identity verification before extending new or additional credit in your name, a security freeze restricts the credit bureaus' ability to release your credit information to third parties without your permission. Security freezes are not available in every state, and may incur an additional charge. The credit bureaus and the FTC can provide you with more information on fraud alerts and security freezes.

- If you need additional information you may contact Bridgewater at One Glendinning Place Westport, CT 06880 or 203.226.3030.