

Nestlé Waters North America Inc.

777 WEST PUTNAM AVENUE
GREENWICH, CT 06830

TEL: 203 863 0534
FAX: 203 863 0250
www.nestlewatersnorthamerica.com



YUN CHOI AU
VICE PRESIDENT AND
DEPUTY GENERAL COUNSEL

February 26, 2008

ARROWHEAD

VIA OVERNIGHT DELIVERY

The Honorable Kelly A. Ayotte
New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

CALISTOGA

Re: Notification of Security Breach Pursuant to N.H. Rev. Stat. §
359-C:20

ICE MOUNTAIN

Dear Madam Attorney General:

Ozarka

This letter is to notify you of a data security breach which may trigger Nestlé Waters North America Inc.'s ("NWNA") notice obligations to you under N.H. Rev. Stat. § 359-C:20.

Zephyrhills

NWNA utilizes a third-party vendor, Systematic Automation Inc. ("SAI"), to create and distribute its employee benefits statements. On February 11, 2008, SAI experienced a break-in at their Fullerton, California facility. According to a police report filed by the Fullerton Police Department, the burglars used a ball bearing to shatter an exterior window of the SAI facility. The thieves proceeded to steal a desktop computer, plus two monitors and flee the scene before authorities arrived in response to the SAI alarm system.



NWNA has learned that the stolen computer contained its 2006 Employee Benefits Statement, which contained sensitive personal information, including names, dates of birth and social security numbers, for approximately 8,245 individuals who were employed by NWNA in 2006. The personal data in the Benefits Statement was not encrypted. However, SAI has informed NWNA that access to the computer's operating system is password protected. At this time, we do not know if the thieves stole the computer with the intent to use the personal information for identity fraud purposes or whether this was merely a random criminal act.



★
S.PELLEGRINO



February 26, 2008

Page 2

Based on our records and information currently available, we believe that the personal information of approximately 61 residents of your state is stored on the stolen computer.

On February 26, 2008, an initial notification was sent by email to all affected employees for whom we had email addresses and was subsequently posted in all NWNA locations. A copy of the notice is enclosed. The notice provides instructions on how individuals can immediately put a fraud alert in place. Additionally, NWNA is working closely with Equifax to set up an emergency response program that will provide any affected individual with 12 months of free credit monitoring services, the option of a "security freeze" on their credit reports, a toll-free information hotline, and information on additional credit monitoring resources.

As soon as the emergency response program is in place, NWNA will send a second notification by US Mail to all affected individuals instructing them on how to utilize the information and credit monitoring resources. NWNA anticipates that the follow-up notification will be sent within the next ten days. Furthermore, NWNA is reviewing its current data security protocols, as well as those of its vendors, to minimize the risk of future security breaches.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Yun Choi Au', written in a cursive style.

Yun Choi Au
Vice President and
Deputy General Counsel

Enclosure

IMPORTANT NOTICE AFFECTING NWNA EMPLOYEES' SENSITIVE PERSONAL INFORMATION. PLEASE READ CAREFULLY.

An Important Notification To Our NWNA Employees:

Systematic Automation Inc. ("SAI"), one of our vendors, recently experienced a break-in at their facility in Fullerton, California. Among other things, a desktop computer was stolen that contained a database of sensitive personal information about NWNA employees, including a list of NWNA employees' names, addresses, dates of birth, and social security numbers. This database only contained information about employees that were on the payroll as of February 1, 2006. If you were not on the payroll at that time, your information was not included in the database. The information was password protected, but was not in an encrypted format.

We use SAI to create and distribute your employee benefits statements. In order for SAI to properly complete the work, we must provide SAI with certain personal information. We deeply regret that this incident occurred and we are taking immediate steps to make sure that something like this does not happen again.

At this time, we do not know if the thieves stole the computer with the intent to use the personal information for credit fraud purposes or whether this was merely a random criminal act. The Fullerton Police Department is investigating the incident and SAI is cooperating fully with the Police Department investigation. If this stolen personal information got in the wrong hands, however, you are at risk for identity theft or fraud.

There are several ways you can minimize the risk of becoming the victim of identity theft and fraud. As an initial matter, you should regularly review your financial account statements and credit cards for any suspicious or unauthorized activity. If you discover any unauthorized activity, immediately report it to your financial institution.

In addition, we recommend that immediately you put a fraud alert in place which is free of charge. This fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a free fraud alert on your credit file, visit: www.fraudalerts.equifax.com or you may contact their auto fraud line at 1-877-478-7625, and follow the prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.

NWNA will also provide, at no cost to you, one year of premium credit monitoring from Equifax, a leading credit monitoring company. We strongly recommend that you sign up for this monitoring program. In the near future, instructions on enrollment will be mailed directly to your homes.

In addition, NWNA is in the process of establishing a hotline to provide you with the resources you need to get your questions answered. This telephone number will also be provided in our follow up mailing. We encourage you to call this number if you have any questions or would like additional information.

NWNA sincerely regrets any inconvenience this incident may cause you. Please rest assured we are taking immediate action to make sure that an incident like this does not happen again and that our valued employees are protected from identity theft and fraud. If you have any immediate questions, please contact your local HR representative.

Sincerely,
Mike Swinton
Vice President, Human Resources
Nestlé Waters North America