

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

DEER
PARK

The Honorable Martha Coakley
Office of the Attorney General
One Ashburton Place
Boston, MA 02108

CALISTOGA

Re: Notification of Security Breach Pursuant to M.G.L.A. 93 H § 3

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 ("NWN") notice obligations to you under M.G.L.A. 93 H § 3.

Poland
Spring

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.

Zephyrhills

Nestlé
PureLife

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.

perrier

PANNA

★
S.PELLEGRINO

Based on our records and information currently available, we believe that the personal information of approximately 495 residents of your state is stored on the stolen computer.

Contrex

February 26, 2008

Page 2

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,



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, Nwana 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.

Nwana 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



KILPATRICK
STOCKTON LLP

Attorneys at Law

Suite 2800 1100 Peachtree St.
Atlanta GA 30309-4530
t 404 815 6500 f 404 815 6555
www.KilpatrickStockton.com

March 11, 2008

direct dial 404 815 6050
direct fax 404 541 3207
HWalker@KilpatrickStockton.com

VIA FEDERAL EXPRESS

Scott D. Schafer
Assistant Attorney General
Consumer Protection Division
The Commonwealth of Massachusetts
Office of the Attorney General
One Ashburton Place
Boston, MA 02108

Re: Nestle Waters North America, Inc.

Dear Scott:

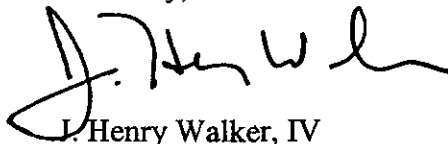
We represent Nestle Waters North America, Inc. ("NWNNA") in connection with a recent data security breach resulting from a computer stolen from one of our vendors. I am responding to your letter dated February 29, 2008 to Yun Choi Au, Vice President and Deputy General Counsel of NWNNA, regarding our notification to Massachusetts' consumers regarding the data security breach.

As we discussed by telephone, the initial email notice we sent to our current employees that was attached to Yun Au's letter dated February 28, 2008 was merely an effort to use the fastest method possible to provide some initial information about the data security breach. NWNNA had always planned to send a primary written notice by U.S. Mail to all affected persons with additional information.

I have attached an example of the written notice that was sent to all Massachusetts residents affected by the data security breach. As you will recall, I sent this notice to you last week and you reviewed and approved it. Based on our conversation, I understand that upon receipt of this notice, your office will close its file related to NWNNA with regard to this data breach notification. I would appreciate a confirmation that the file has been closed.

Thank you for your cooperation in this matter. Please call me if you would like to discuss this matter further.

Sincerely,



J. Henry Walker, IV

JHW/cp
Encl.

Nestle Waters North America
777 West Putnam Avenue
Greenwich, CT 06830



IMPORTANT NOTICE REGARDING CURRENT AND FORMER NWNA EMPLOYEES' SENSITIVE PERSONAL INFORMATION. PLEASE READ CAREFULLY.



WAKEFIELD MA 01880-1227



Promotion Code : 30114-1814672793

March 07, 2008

An Important Notification To Current and Former 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 did not include credit card or bank account information. It 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.

If you suspect you are a victim of identify theft or fraud, you should immediately report the crime to your law enforcement and the FTC (1-877-ID-THEFT). You have a right to obtain a police report regarding the suspected crime.

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

10000000000000

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 Equifax Credit Watch™ Gold with 3-in-1 Monitoring. Equifax Credit Watch Gold with 3-in-1 Monitoring will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your credit files at Equifax, Experian and Trans Union. The key features and benefits of the 1 year subscription to Equifax Credit Watch Gold with 3-in-1 Monitoring that is being offered to you are:

1. Comprehensive credit file monitoring with instant alerts of key changes to your Equifax, Experian, and Trans Union credit reports
2. Free 3-in-1 Credit Report available when you enroll and unlimited access to your Equifax Credit Report™
3. Up to \$20,000 Identity Theft Insurance with no deductible (excludes NY residents) at no additional charge to you
4. Customer Care 24 hours a day, 7 days a week

Attached are instructions on how to enroll with Equifax. We strongly recommend that you contact Equifax and sign up for this product. Please take a few minutes now and enroll. You will need to enroll within 90 days of receiving this letter.

You also have a right to request a "security freeze" on your consumer report. More information about a security freeze and how to obtain one is also attached.

In addition, NWNA has established a hotline to provide you with the resources you need to get your questions answered. The hotline telephone number is 1-800-697-1132 and is available Monday through Friday, 9am to 9pm, Eastern Standard Time. 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 current and former employees are protected from identity theft and fraud.

Sincerely,



Mike Swinton
Vice President, Human Resources
Nestlé Waters North America

000100-000001

Equifax Credit Watch™ Gold with 3-in-1 Monitoring

How to Enroll

Equifax has a simple Internet-based verification and enrollment process.

Visit: www.myservices.equifax.com/tri

1. **Consumer Information:** complete the form with your contact information (name, address and e-mail address) and click "Continue" button. The information is provided in a secured environment.
2. **Identity Verification:** complete the form with your Social Security Number, date of birth, telephone #s, create a User Name and Password, agree to the Terms of Use and click "Continue" button. The system will ask you up to two security questions to verify your identity.
3. **Payment Information:** During the "check out" process, provide the promotion code provided in your letter in the "Enter Promotion Code" box. (no spaces, include dash, case sensitive.) After entering your code press the "Apply Code" button and then the "Submit Order" button at the bottom of the page. (This code eliminates the need to provide a credit card number for payment.)
4. **Order Confirmation:** - Click "View My Product" to access your 3-in-1 Credit Report.

To sign up for US Mail delivery of the product, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. **Promotion Code:** enter your promotion code provided in your letter (no spaces, **no dash**)
2. **Customer Information:** enter your home telephone number, home address, name, date of birth and Social Security Number.
3. **Permissible Purpose:** provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax can not process your enrollment.
4. **Order Confirmation:** Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided).

1000000-001000

NOTICE ABOUT YOUR RIGHT TO REQUEST A SECURITY FREEZE

You have a right to request a "security freeze" on your consumer report. The security freeze will prohibit a consumer reporting agency from releasing any information in your consumer report without your express authorization. A security freeze can be requested by sending a request either by certified mail, overnight mail or regular stamped mail to a consumer reporting agency with the following information.

1. Your name
2. Current address and previous addresses for the past two years
3. Date of birth
4. Social Security Number
5. Copy of a government issued identification card, such as a driver's license, state or military ID card,
6. Proof of current address such as a current utility bill
7. Payment of applicable fees to request a security freeze of your credit file. (Cost varies by state. For Massachusetts residences, a security freeze is \$5 or free for identity theft victims with a valid law enforcement report).

The address for each consumer reporting agency is below.

Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

TransUnion Fraud Victim Assistance
P.O. Box 6790
Fullerton, CA 92834

The security freeze is designed to prevent credit, loans or services from being approved in your name without your consent. You should be aware that using a security freeze may delay, interfere with, or prevent the timely approval of any subsequent request or application you make regarding new loans, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular phone, utilities, digital signature, internet credit card transactions, or other services, including an extension of credit at point of sale.

When you place a security freeze on your consumer report, within 5 business days of receiving your request for a security freeze, the consumer reporting agency should provide you with a personal identification number or password to use if you choose to remove the freeze on your consumer report or to authorize the release of your consumer report to a specific party or for a specified period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide the following:-

- (1) the personal identification number or password provided by the consumer reporting agency;
- (2) proper identification to verify your identity; and

000100-000001

(3) the third party or parties who are to receive the consumer report or the specified period of time for which the report shall be available to authorized users of the consumer report.

A consumer reporting agency that receives a request from a consumer to lift a freeze on a consumer report should comply with the request not later than 3 business days after receiving the request.

A security freeze should not apply to a person or entity, or to its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account, that requests information relative to your consumer report for the purposes of reviewing or collecting the account, if you have previously given consent to the use of your consumer report. "Reviewing the account" includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

000100-000001