

MERCER

March 15, 2011

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

Re: Legal Notice of Potential Information Security Breach

Dear Attorney General:

We are writing to advise you of an incident involving personal information associated with 1 resident of the State of New Hampshire. Mercer Administration, a service of Seabury & Smith, Inc. ("Mercer Administration") provides health and welfare benefit administration services to Sperian Protection USA Inc. ("Sperian"). Mercer mistakenly provided access to a Sperian billing folder on a proprietary database to one of Sperian's medical insurance carriers. This billing folder contained encrypted personal information which may have included name, SSN and dollar amount for health election premiums. A carrier user inadvertently accessed Sperian's consolidated billing folder on January 27, 2011. The user immediately realized that she had accessed information related to Sperian employees not covered by the carrier, closed out of the folder and contacted Mercer to report the issue.

Mercer Administration notified Sperian, the information owner, promptly of this incident. Mercer Administration promptly acted to (1) remedy this incident by terminating the unintended carrier access and (2) investigate and analyze the potential impact. This investigation and analysis consisted of determining potentially impacted participants and state notification requirements as well as investigating the impact of the existing relationship between the client and the carrier, as the carrier does provide some services to the client, which resulted in a gap between date of notification and discovery of breach. Mercer Administration promptly notified Sperian of the results of its investigation and analysis.

The carrier user notified Mercer Administration of the inappropriate access and promptly closed out of the folder. Neither Mercer Administration nor Sperian has knowledge or reason to believe that any information of Sperian employees has been misused or accessed by any third parties.

Mercer Administration takes privacy and information security seriously. In order to ensure that potentially affected individuals are able take to steps to protect themselves from possible identity theft or other damage, Mercer Administration, on behalf of itself and Sperian will be alerting these individuals about the situation this week. We will alert individuals to remain vigilant by reviewing account statements and monitoring free credit reports.

Mercer Administration is taking steps to help ensure this situation is not repeated. Mercer Administration will also be notifying the three major credit reporting repositories (Experian, Equifax and TransUnion).

Please let us know if you have further questions.

Sincerely,



Constantine Karbaliotis, J.D., CIPP/C/IT
Americas Privacy Leader
Mercer
c/o Carolyn Parziale
1 Investors Way
Norwood, MA 02062

Enclosure

| MERCER

Dear <<FirstName>> <<LastName>>,

We are writing to inform you of an incident involving your personal information. Sperian Protection USA, Inc. ("Sperian") has a contract with Mercer Administration, a service of Seabury & Smith, Inc. ("Mercer Administration"). The incident occurred when Mercer mistakenly provided access to a Sperian billing folder on a proprietary Mercer database to one of Sperian's medical insurance carriers. This billing folder contained encrypted personal information which may have included your name, SSN and dollar amount for health election premium.

A carrier inadvertently accessed Sperian's consolidated billing folder on January 27, 2011. The user immediately realized that she had accessed information related to Sperian employees not covered by the carrier, closed out of the folder and contacted Mercer to report the issue.

Neither Mercer nor Sperian has knowledge or reason to believe that your personal information has been misused and because of the extremely limited nature of this vulnerability we believe that any improper use is very unlikely. Nevertheless, we wanted to make you aware of the incident and the steps we have taken to prevent a reoccurrence. First, Mercer conducted an investigation of this regrettable incident and promptly worked to terminate the unintended carrier access. Second, Mercer has notified state regulators, as appropriate, and the three national credit bureaus of this incident. Additionally, Mercer is taking steps to provide greater protection for personal information.

Mercer is committed to the protection of your privacy and personal information. Therefore, in addition to the measures above, we are providing you the attached document entitled U.S. State Notification Requirements. This document contains information on how to contact the credit repositories (Experian, Equifax and TransUnion) if you so choose.

Even though Mercer has taken the actions outlined in this letter and believes that the risk of potential identity theft is low, we nevertheless recommend that you remain vigilant and review your account statements and credit reports regularly. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report fraudulent activity or any suspected incidence of identity theft to proper local law enforcement authorities.

Again, Mercer apologizes for any inconvenience this may have caused. If you have questions, please call contact Debix between at 512-579-2471 or toll free at 1-877-403-0237 between 9:00 AM and 5:00 PM (Central Time), Monday through Saturday.

Sincerely,

Constantine Karbaliotis, J.D., CIPP/C/IT
Americas Privacy Leader
Mercer

Enclosure

U.S. State Notification Requirements

For residents of Hawaii, Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, Vermont, Virginia, West Virginia, and Wyoming

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on our account. It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax

P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19022
1-800-888-4213
www.transunion.com

For residents of Iowa

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Maryland and North Carolina

You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about steps you can take to avoid identity theft.

Maryland Office of the Attorney General

Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

North Carolina Office of the Attorney General

Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission

Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/bcp/edu/microsites/idtheft

For residents of Massachusetts and West Virginia

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft. You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit.

To place a security freeze on your credit report, you need to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to \$5.00 to place, lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 303748
www.equifax.com

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion (FVAD)

P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com