



June 17, 2013

Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

To whom it may concern:

Pursuant to RSA 359-C:20 and on behalf of Apria Healthcare Group Inc., we are writing to notify you of an unauthorized disclosure of personal information involving one New Hampshire resident.

On April 26, 2013, a Fidelity associate inadvertently included information about one participant in the Apria Healthcare plan in a report that was intended for another plan sponsor client firm. The report was attached to a secure, encrypted e-mail and sent to the other plan sponsor client firm. The information about the plan participant included name and Social Security number. No other personal information about the participant was included in the attached report. Three employees at the other client firm had access to this email and the attached report. These employees included a benefits manager and two employees within the IT department, all of whom are authorized to handle personal information for their firm's plan as part of their job responsibilities.

Fidelity became aware of this matter on May 10, 2013. We immediately began to research this matter and on May 13, 2013, at our request, the recipients deleted this information. Upon learning of this incident, Fidelity handled the matter in accordance with its internal procedures. Law enforcement was not notified because there was no evidence of fraudulent activity or misuse of the information. Fidelity will be taking steps to further strengthen its administrative control procedures to help prevent a recurrence.

This incident impacted one New Hampshire resident. We notified the residents by letter on June 17, 2013. A copy of the notification letter is attached. While the risk associated with this matter appears minimal and we are not aware of any misuse of this information, as a precautionary measure, Fidelity has offered those affected a free subscription to a credit monitoring service for one year.

If you have any questions, please contact William Duserick, Chief Privacy Officer, Fidelity Investments, at 617-392-1224.

Sincerely,

A handwritten signature in black ink that reads "William G. Duserick". The signature is written in a cursive, flowing style.

William G. Duserick
Chief Privacy Officer
Fidelity Investments

Attachment



June 17, 2013

Participant
Street Address
City, ST Zip+four

We are writing in regard to a matter that involved some personal information about you held by Fidelity Investments, a retirement plan administrative service provider for the [Plan Name]. On April 26, 2013, information about you was inadvertently included in a retirement plan report sent by secure, encrypted email to another Fidelity retirement services client firm. The report included your name and Social Security number. No other personal information about you was included in the report. Three employees at the Fidelity client firm had access to this report, including a benefits manager and two employees within the IT department. These employees are authorized to handle personal data related to their firm's benefits plans as part of their job responsibilities and fully cooperated with Fidelity in the return and deletion of the report. We are not aware of any misuse of this information nor do we expect any.

Fidelity became aware of this matter on May 10, 2013. We immediately began to research this matter and at our request, on May 13, 2013, the recipients deleted the information about you. Please know that we take the protection of your information very seriously and have taken steps to further strengthen our administrative control procedures to help prevent a recurrence.

While we are not aware of any misuse of this information, it's always a good idea to regularly review your account statements, monitor your credit reports, and promptly report any activity of concern. And while the risk associated with this matter appears minimal, as a precautionary measure, Fidelity has arranged for you to enroll, at your option, in a credit monitoring service for one year at no cost to you. This service allows you to monitor your credit and to detect any unusual activity that may affect your personal financial situation. The service is provided by Equifax, a major credit reporting company. For details on how to enroll in this service and for additional ways you may protect yourself, please refer to the enclosed instruction sheet.

We sincerely apologize for any concern or inconvenience this matter may cause you. If you have any questions regarding this situation, please feel free to call Fidelity at 1-xxx-xxx-xxxx.

Sincerely,

A handwritten signature in black ink that reads 'William S. Duserick'.

William Duserick
Chief Privacy Officer

ADDITIONAL STEPS TO PROTECT YOURSELF

Directions for Placing a Fraud Alert

You may want to consider placing an initial fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies. The agency that processes your fraud alert will notify the other two credit reporting agencies on your behalf. An initial fraud alert stays on your credit report for 90 days. When you place this alert on your credit report, you will receive information about ordering one free credit report from each of the credit reporting companies. Once you receive your reports, review them carefully for inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain. Verify the accuracy of your Social Security number, address(es), full name and employer(s). Notify the credit reporting companies if any information is incorrect.

You may also contact the three nationwide credit reporting agencies to place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

Equifax: 877-478-7625 www.equifax.com; PO Box 740241, Atlanta, GA 30374-0241

Experian: 888-397-3742 www.experian.com; PO Box 9532, Allen, TX 75013

TransUnion LLC: 800-680-7289 www.transunion.com; PO Box 6790, Fullerton, CA 92834

Directions for Obtaining a Credit Report

Please remember that while this matter may not involve significant risk, it is always good practice to take sensible steps to remain vigilant and protect yourself by regularly reviewing your account statements and your credit report for incidents of fraud and identity theft. Report suspected incidents of identity theft to local law enforcement or to your state attorney general. As you may know, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the major credit reporting agencies. You may obtain a free copy of your credit report by calling 1-877-FACT ACT (1-877-322-8228) or by visiting www.annualcreditreport.com.

Resources

Additional information on identity theft, fraud alerts, security freezes and other protections you can take is available from the Federal Trade Commission (FTC). You may contact the FTC to report any incidents of identity theft and to obtain guidance about protecting against identity theft.

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

Toll-free Identity Theft Helpline: 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261

Website: www.ftc.gov/bcp/edu/microsites/idtheft/