



July 31, 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 Oracle Corporation, we are writing to notify you of an unauthorized disclosure of personal information involving 472 New Hampshire residents. Fidelity is a retirement plan administrative service provider for Oracle.

On July 10, 2013, information about Oracle employees was inadvertently included in a report that was briefly viewed by a plan administrator at another Fidelity client firm. The report was only accessible through a password-protected application and only one employee at the Fidelity client firm had access to this report, a Human Resources manager, who is authorized to handle personal data related to his firm's benefits plans as part of his job responsibilities. The report included the following information about the employees: name, Social Security number, compensation, and other information related to administration of the 401(k) savings and investment plan.

Fidelity became aware of this matter on July 10, 2013, and immediately deleted the report from the password-protected application. The recipient fully and promptly cooperated with Fidelity in the deletion of the report. We have taken steps to further strengthen our administrative control procedures to help prevent a recurrence.

This incident impacted 472 New Hampshire residents. We will be notifying the residents by letter on August 1, 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, Fidelity is prepared to offer a free subscription to a credit monitoring service for one year for Oracle employees who contact Fidelity with further questions about the matter.

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".

William G. Duserick
Chief Privacy Officer
Fidelity Investments

Attachment



July 31, 2013

Participant Name
Street
City, State Zip

Dear Current or Former Oracle Employee:

We are writing to notify you of a matter that involved some information about you held by Fidelity Investments, a retirement plan administrative service provider for Oracle Corporation.

On July 10, 2013, information about you was inadvertently included in a report that was briefly viewed by a plan administrator at another Fidelity client firm. The report included your name, Social Security number, compensation, and other information related to administration of your 401(k) savings and investment plan. The report that contained this information was only accessible through a password-protected application and only one employee at the Fidelity client firm had access to this report, a Human Resources manager, who is authorized to handle personal data related to his firm's benefits plans as part of his job responsibilities. That employee fully and promptly cooperated with Fidelity in the return and deletion of the report. While we are not aware of any misuse of this information nor do we expect any, it is always a good idea to remain vigilant and regularly review your account statements, monitor your credit reports, and promptly report any activity of concern.

Fidelity became aware of this matter on July 10, 2013, and immediately deleted the report from the password-protected application. 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.

We sincerely apologize for any concern of inconvenience this matter may cause you. If you have any questions regarding this matter, please feel free to call Fidelity at 1-800-410-2363.

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/

Maryland Residents:

Additional information about steps to avoid identity theft is available from the following source:

Maryland Attorney General's Office

Identity Theft Unit

200 St. Paul Place

Baltimore, MD 21202

Phone: 1-888-743-0023

<http://www.oag.state.md.us/>

North Carolina Residents:

Additional information about steps to prevent identity theft is available from the following source:

North Carolina Office of the Attorney General

Consumer Protection Division

9001 Mail Service Center

Raleigh, NC 27699-9001

Telephone: 1-877-566-7226

Website: www.ncdoj.com/Protect-Yourself/2-4-3-Protect-Your-Identity.aspx