

Hewlett-Packard Company
3404 E. Harmony Road
Mail Stop 79
Ft. Collins, CO 80528
www.hp.com

Kathryn S. Young
Senior Counsel
303.955.3283 Tel
970.898.7247 Fax
kyoung@hp.com

16 August 2007
VIA FACSIMILE AND OVERNIGHT MAIL

New Hampshire Department of Justice
Office of the Attorney General
Consumer Protection & Antitrust Bureau
33 Capital Street
Concord, NH 03301
Fax #: (603)271-2110

RE: Data Breach Notification

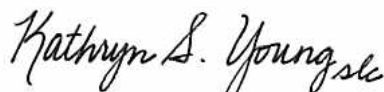
To Whom It May Concern:

In accordance with N.H. Rev. Stat. § 359-C:201.(b), we are providing you with written notification regarding the nature and circumstances of a laptop loss that may have resulted in the compromise of personal information of some **Mercury Interactive**¹ former employees. We are working with law enforcement authorities to recover the lost laptop.

The loss of the laptop may have compromised certain personal information of 1425 former employees of Mercury Interactive, including 10 New Hampshire residents. The information that may have been compromised includes name, address and social security number. At this time, we have no evidence that any information has been used to commit identity fraud. As indicated above, we have notified law enforcement authorities about this loss.

Attached for your information is a sample of the breach notification letter we are sending to affected individuals on or about August 17, 2007. If you have any questions, please do not hesitate to contact me at **303-955-3283**.

Very truly yours,



Kathryn S. Young

¹ Mercury Interactive was acquired by Hewlett-Packard Company in November 2006.



Hewlett-Packard Company
HP Privacy Office
3000 Hanover Street
Mail Stop 1114
Palo Alto, CA 94304

August 17, 2007

Notification of Potential Data Breach

To former employees of Mercury Interactive,

We recently became aware of an incident involving personal information that may affect you. A laptop belonging to an HP director was lost during a business trip to Atlanta in late July. The laptop contained personal information including names, Social Security numbers, addresses, dates of birth, citizenship, and compensation information.

The laptop was secured by a user name/password combination. Although we have no reason to believe that any of the information has been accessed or misused, law enforcement has been notified and is attempting to find the laptop.

We take our obligation to safeguard your personal information very seriously and, therefore, we are alerting you so you can take steps to protect yourself from identity fraud.

Hewlett-Packard is contacting the three principle credit reporting bureaus, Equifax, Experian, and TransUnion, to advise them of this situation. In addition, Hewlett-Packard has also arranged for you to enroll, at your option, in a credit monitoring service at no cost to you. This service will allow you to monitor your credit as well as any unusual activity that may affect your personal financial situation. The service is provided by Equifax, one of the major credit reporting companies that monitors activity.

To enroll in the service, follow the instructions in the attached document. You may either enroll on line using the promotional code provided, or you may call Equifax at 1-866-937-8482. Once you have enrolled, you will be provided with several valuable services including credit monitoring, a copy of your credit report, notification of activity, and additional access to your credit report. In addition, you will have access to Equifax's customer service representatives.

In addition, you are entitled under U.S. law to one free credit report annually from each of the three national credit bureaus. To order your free annual credit report from one or all of the national credit reporting companies, visit www.annualcreditreport.com, call toll-free 877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, PO Box 105281, Atlanta, GA 30348-5281. You can print the form from www.ftc.gov/credit. Do not contact the three nationwide credit reporting companies individually. And if you ask, only the last four digits of your Social Security number will appear on your credit reports.

You may also want to place a 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 call any one of the three major credit reporting companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.

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), complete name and employer(s). Notify the credit reporting companies if any information is incorrect.

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: 800-680-7289 www.transunion.com; Fraud Victim Assistance Division, PO Box 6790, Fullerton CA 92834-6790

We recommend that you check your credit reports and review your account statements periodically. This can help you spot problems and address them quickly. If you believe that you are a victim of identity theft, you should notify your local law enforcement agency and the Federal Trade Commission. You may contact the Federal Trade Commission by calling their hotline phone number at 1-877-IDTHEFT (438-4338) or by visiting their website at www.ftc.gov.

If you believe your identity has been stolen, the Federal Trade Commission ("FTC") recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.
- File your concern with the FTC. The FTC maintains a database of identity theft cases used by law enforcement agencies for their investigations. Filing a concern helps the FTC learn more about identity theft and the problems victims are having.

Please know that Hewlett-Packard is treating this matter extremely seriously and deeply regrets this situation.

If you require additional information you may contact the Hewlett-Packard Privacy Office by sending an email message to privacy@hp.com or by calling 281-518-0208

Sincerely,

Scott Taylor
Chief Privacy Officer
Hewlett-Packard Company