

RECEIVED  
OFFICE OF THE ATTORNEY GENERAL  
2009 JAN 16 P 1:41



Hewlett-Packard Company  
200 Forest Street  
Marlborough, MA 01752  
www.hp.com

Paul Henrion  
Legal Department  
Hewlett-Packard Company

1.508.467.4018 Tel  
1.508.467.4022 Fax  
paul.henrion@hp.com

January 15, 2009

Office of the Attorney General  
200 St. Paul Place  
Baltimore, MD 21202  
Fax: 410.576.6566

RE: Data Security Incident

To Whom It May Concern:

In accordance with Md. Ann. Code § 14-3504, we are writing to update you on the theft of a laptop computer containing certain personal information about some participants in HP benefits programs. We previously notified you of this theft by letter dated December 3, 2008. We have now learned that the laptop included information such as names, Social Security numbers, medical history, diagnosis or treatment, and health insurance account numbers of some current and former employees. At this time, we are aware of approximately 601 Maryland residents who may be affected by this incident beyond the 626 residents in our prior notice to you. We are taking steps to help ensure that this type of incident does not happen in the future.

Attached for your information are samples of the notices we are sending to affected individuals both those previously notified and those newly notified. Also attached for your information is a copy of our prior notice to you. If you have any questions, please do not hesitate to contact me.

Sincerely,

Paul Henrion  
Privacy Counsel





Hewlett-Packard Company  
3000 Hanover Street  
Palo Alto, CA 94304-1112

January X, 2009

[Name]  
[Address]  
[Address]

Dear Participant:

I am writing to inform you of the theft of a laptop computer which contained certain personal information of some participants in the HP benefits program. Although there is no evidence to suggest that the information on the laptop has been misused, HP has been working closely with law enforcement authorities to recover the laptop, which was stolen several months ago.

We have been working to fully establish the specific information contained on the laptop and information such as names, Social Security numbers, medical history, diagnosis or treatment, and health insurance account numbers of some current and former employees have been identified. Steps are being taken to help ensure that this type of incident does not happen in the future.

We regret that this incident may affect you. We take our obligation to safeguard personal information very seriously and, therefore, we are alerting you so you can take steps to help protect yourself from possible identity theft. The laptop was secured by a user name and password, and we have no evidence indicating that any of the information has been accessed or misused. Nevertheless, we encourage you to remain vigilant for incidents of identity theft and to regularly review and monitor your account statements and credit reports. The reverse side of this letter and the attached Reference Guide provides details on these and other actions you may wish to consider.

We recommend that you regularly review your medical statements (including your "Explanation of Benefits" statements), and check for charges you do not recognize. You may want to keep a copy of this letter in case of future issues with your medical records.

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 credit reports, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free (877) 322-8228.

To further assist you, we are offering you the opportunity to enroll in credit monitoring, which we have arranged to provide at no charge to you for up to two years. The reverse side of this letter provides information on how you can enroll in Triple Alert<sup>SM</sup> credit monitoring. The attached Reference Guide also includes recommendations by the U.S. Federal Trade Commission on how to further protect yourself against identity theft. You may also want to place a fraud alert or security freeze on your credit file.

If you require additional information you may contact the Hewlett-Packard Privacy Office by sending an email message to [privacy@hp.com](mailto:privacy@hp.com) or by calling (800) 335-6278.

Again, we regret any inconvenience this may cause you and will continue to pursue this matter to help prevent this type of incident from occurring in the future.

Sincerely,

Scott Taylor

Chief Privacy Officer  
Hewlett-Packard Company

**To Enroll in the Credit Monitoring Product:**

To help you detect the possible misuse of your personal information, we are providing you with a complimentary two year membership in the Triple Alert<sup>SM</sup> credit monitoring product at no cost to you. Triple Alert<sup>SM</sup> will be provided by ConsumerInfo.com, Inc., an Experian<sup>®</sup> company and will monitor your credit reports at the three national credit reporting companies: Experian, Equifax<sup>®</sup> and TransUnion<sup>®</sup> and notify you of key changes. Triple Alert<sup>SM</sup> is a powerful tool that will help you identify potentially fraudulent use of your information. Your Triple Alert<sup>SM</sup> membership is completely free and will not hurt your credit score.

The complimentary 24-month **Triple Alert<sup>SM</sup>** membership includes:

- Daily monitoring of your credit reports every day so you don't have to
- Notification alerts when key changes are detected so you can act quickly
- If you become a victim of fraud or identity theft, a Fraud Resolution Representative will assist you with the process of resolving problems associated with credit fraud or identity theft
- \$25,000 in identity theft insurance provided by Virginia Surety Company, Inc. with no deductible\*

\*Due to New York state law restrictions, identity theft insurance coverage cannot be offered to residents of New York. All other benefits of Triple Alert<sup>SM</sup> are available to residents of New York.

You have until March 27, 2009 to activate this membership, which will then continue for 24 full months. We encourage you to activate your credit monitoring membership as soon as possible.

The web site to enroll in Triple Alert and your individual activation code are both listed below. To sign up, please visit the web site and enter your individual activation code. Please keep in mind that once activated, the code cannot be re-used for another enrollment. The web site will guide you through the process of enrolling in Triple Alert. If you need technical assistance, please call customer care toll free at (866) 252-0121 (or direct dial outside the U.S. at (479) 573-7373).

Triple Alert Web Site: <http://partner.consumerinfo.com/hp>

Your Activation Code: **[insert Activation Code using required 14-point font]**

If you wish to enroll over the phone for delivery of your membership via US mail, please call customer care toll free at (866) 252-0121 (or direct dial outside the U.S. at (479) 573-7373).

Again, your Triple Alert membership is completely free and will not hurt your credit score.

## Reference Guide

We encourage individuals receiving Hewlett-Packard's letter to take the following steps:

**Order Your Free Credit Reports.** To order your free credit reports, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at [www.ftc.gov](http://www.ftc.gov) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually. They provide free annual credit reports only through the website or toll-free number.

When you receive your credit report, review it carefully and look for accounts you don't recognize. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in the information (such as your home address and Social Security number). Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

If you find items you don't understand on your report, call the credit bureaus at the number given on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

**Contact the U.S. Federal Trade Commission.** If you detect any unauthorized transactions in your financial account, promptly notify your financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission. If you believe your identity has been stolen, the U.S. 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](http://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.

You can learn more about how to protect yourself from becoming a victim of identity theft by contacting the FTC:

- Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
[www.ftc.gov/idtheft/](http://www.ftc.gov/idtheft/)

**Place a Fraud Alert on Your Credit File.** To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity

theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

- Equifax P.O. Box 740241 800-525-6285 www.equifax.com  
Atlanta, Georgia 30374-0241
- Experian P.O. Box 9532 888-397-3742 www.experian.com  
Allen, Texas 75013
- TransUnion Fraud Victim Assistance Division 800-680-7289 www.transunion.com  
P.O. Box 6790  
Fullerton, California 92834-6790

**Place a Security Freeze on Your Credit File.** You may wish to place a “security freeze” on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze by contacting each of the three credit bureaus at:

- Equifax P.O. Box 105788 www.equifax.com  
Atlanta, Georgia 30348
- Experian P.O. Box 9554 www.experian.com  
Allen, Texas 75013
- TransUnion Fraud Victim Assistance Division www.transunion.com  
P.O. Box 6790  
Fullerton, California 92834-6790

The credit bureaus may charge a reasonable fee to place a freeze on your account and may require that you provide proper identification prior to honoring your request.

- **For Maryland Residents.** You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at:

Maryland Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
888-743-0023  
www.oag.state.md.us



January X, 2009



Hewlett-Packard Company  
3000 Hanover Street  
Palo Alto, CA 94304-1112

[Name]  
[Address]  
[Address]

Dear Participant:

I am writing to update you on the theft of a laptop computer which contained certain personal information of some participants in the HP benefits program. You were previously mailed a notice concerning this theft earlier in December. Although there continues to be no evidence to suggest that the information on the laptop has been misused, we would like to update you on additional information discovered through a review of files contained on the laptop.

In addition to the previously identified names and Social Security numbers, we have identified additional information through a review of the files contained on the laptop such as medical history, diagnosis or treatment, and health insurance account numbers of some current and former employees. Steps are being taken to help ensure that this type of incident does not happen in the future.

We regret that this incident may affect you. We are alerting you of the updated information so you can take steps to help protect yourself from possible identity theft or other misuse of information. The original notice you were mailed provided information on enrollment in credit monitoring for up to two years at no charge, placing a fraud alert or security freeze on your credit file and other resources you can use to seek additional protections or information.

Because some health-related information (described above) was contained on the laptop, we also recommend that you regularly review your medical statements (including your "Explanation of Benefits" statements) and check for charges you do not recognize. You may want to keep a copy of this letter in case of future issues with your medical records.

If you require additional information you may contact the Hewlett-Packard Privacy Office by sending an email message to [privacy@hp.com](mailto:privacy@hp.com) or by calling (800) 335-6278.

Again, we regret any inconvenience this may cause you and will continue to pursue this matter to help prevent this type of incident from occurring in the future.

Sincerely,

Scott Taylor  
Chief Privacy Officer  
Hewlett-Packard Company



\* \* \* COMMUNICATION RESULT REPORT ( DEC. 3. 2008 1:20PM ) \* \* \*

FAX HEADER: HP

TRANSMITTED/STORED : DEC. 3. 2008 1:19PM  
FILE MODE OPTION

ADDRESS

RESULT

PAGE

363 MEMORY TX

914105766566

OK

6/6

REASON FOR ERROR  
E-1) HANG UP OR LINE FAIL  
E-3) NO ANSWER

E-2) BUSY  
E-4) NO FACSIMILE CONNECTION



Corporate Legal Department  
Hewlett-Packard Company  
3000 Hanover Street MS 1050  
Palo Alto CA 94304-1112  
650.857.8474 Fax

<b>To</b>	<b>Company</b>
Office of the Attorney General	State of Maryland
<b>From</b>	<b>Subject</b>
Paul Henrion	Data Security Incident

<b>Telephone</b>	<b>Fax</b>
	410.576.6566
<b>Number of Pages</b>	<b>Date</b>
	December 3, 2008

Warning: This message is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential, and exempt from disclosure under applicable law. If you are not the intended recipient, you are hereby notified that any use, dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone, and return this original message to us at the above address via the U.S. Postal Service. Thank you



Hewlett-Packard Company  
200 Forest Street  
Marlborough, MA 01752  
www.hp.com

Paul Henrion  
Legal Department  
Hewlett-Packard Company  
1.508.467.4018 Tel  
1.508.467.4022 Fax  
paul.henrion@hp.com

December 3, 2008

Office of the Attorney General  
200 St. Paul Place  
Baltimore, MD 21202  
Fax: 410.576.6566

RE: Data Security Incident

To Whom It May Concern:

In accordance with Md. Ann. Code § 14-3504, we are writing to inform you of the theft of a laptop computer containing certain personal information about some participants in HP benefits programs. The information on the laptop included names and Social Security numbers of some current and former employees. We are working with law enforcement authorities to recover the stolen laptop. At this time, we are aware of approximately 626 Maryland residents who may be affected by this incident. (We are continuing to investigate what information was contained on the laptop) and, to the extent further notification is required, we will notify affected residents and provide you with an update. We are taking steps to help ensure that this type of incident does not happen in the future.

Attached for your information is a sample of the notice we are sending to affected individuals. If you have any questions, please do not hesitate to contact me.

Sincerely,

Paul Henrion  
Privacy Counsel



Hewlett-Packard Company  
3000 Hanover Street  
Palo Alto, CA 94304-1112

December X, 2008

[Name]  
[Address]  
[Address]

Dear Participant:

I am writing to inform you of the theft of a laptop computer which contained certain personal information of some participants in the HP benefits program. Although there is no evidence to suggest that the information on the laptop has been misused, HP has been working closely with law enforcement authorities to recover the laptop, which was stolen several months ago.

We have been working to fully establish the specific information contained on the laptop and, at this time, names and Social Security numbers of some current and former employees have been identified. Steps are being taken to help ensure that this type of incident does not happen in the future.

We regret that this incident may affect you. We take our obligation to safeguard personal information very seriously and, therefore, we are alerting you so you can take steps to help protect yourself from possible identity theft. The laptop was secured by a user name and password, and we have no evidence indicating that any of the information has been accessed or misused. Nevertheless, we encourage you to remain vigilant for incidents of identity theft and to regularly review and monitor your account statements and credit reports. The reverse side of this letter and the attached Reference Guide provides details on these and other actions you may wish to consider.

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 credit reports, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free (877) 322-8228.

To further assist you, we are offering you the opportunity to enroll in credit monitoring, which we have arranged to provide at no charge to you for up to two years. The attached Reference Guide provides information on how you can enroll in Triple Alert<sup>SM</sup> credit monitoring and recommendations by the U.S. Federal Trade Commission on how to further protect yourself against identity theft. You may also want to place a fraud alert or security freeze on your credit file.

If you require additional information you may contact the Hewlett-Packard Privacy Office by sending an email message to [privacv@hp.com](mailto:privacv@hp.com) or by calling (800) 335-6278.

Again, we regret any inconvenience this may cause you and will continue to pursue this matter to help prevent this type of incident from occurring in the future.

Sincerely,

Scott Taylor  
Chief Privacy Officer  
Hewlett-Packard Company

**To Enroll in the Credit Monitoring Product:**

To help you detect the possible misuse of your personal information, we are providing you with a complimentary two year membership in the Triple Alert<sup>SM</sup> credit monitoring product at no cost to you. Triple Alert<sup>SM</sup> will be provided by ConsumerInfo.com, Inc., an Experian<sup>®</sup> company and will monitor your credit reports at the three national credit reporting companies: Experian, Equifax<sup>®</sup> and TransUnion<sup>®</sup> and notify you of key changes. Triple Alert<sup>SM</sup> is a powerful tool that will help you identify potentially fraudulent use of your information. Your Triple Alert<sup>SM</sup> membership is completely free and will not hurt your credit score.

The complimentary 24-month Triple Alert<sup>SM</sup> membership includes:

- Daily monitoring of your credit reports every day so you don't have to
- Notification alerts when key changes are detected so you can act quickly
- If you become a victim of fraud or identity theft, a Fraud Resolution Representative will assist you with the process of resolving problems associated with credit fraud or identity theft
- \$25,000 in identity theft insurance provided by Virginia Surety Company, Inc. with no deductible\*

\*Due to New York state law restrictions, identity theft insurance coverage cannot be offered to residents of New York. All other benefits of Triple Alert<sup>SM</sup> are available to residents of New York.

You have until February 28, 2009 to activate this membership, which will then continue for 24 full months. We encourage you to activate your credit monitoring membership as soon as possible.

The web site to enroll in Triple Alert and your individual activation code are both listed below. To sign up, please visit the web site and enter your individual activation code. Please keep in mind that once activated, the code cannot be re-used for another enrollment. The web site will guide you through the process of enrolling in Triple Alert. If you need technical assistance, please call customer care toll free at (866) 252-0121 (or direct dial outside the U.S. at (479) 573-7373).

Triple Alert Web Site: <http://partner.consumerinfo.com/hp>

Your Activation Code: **[insert Activation Code using required 14-point font]**

If you wish to enroll over the phone for delivery of your membership via US mail, please call customer care toll free at (866) 252-0121 (or direct dial outside the U.S. at (479) 573-7373).

Again, your Triple Alert membership is completely free and will not hurt your credit score.

## Reference Guide

We encourage individuals receiving Hewlett-Packard's letter to take the following steps:

**Order Your Free Credit Reports.** To order your free credit reports, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at [www.ftc.gov](http://www.ftc.gov) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually. They provide free annual credit reports only through the website or toll-free number.

When you receive your credit report, review it carefully and look for accounts you don't recognize. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in the information (such as your home address and Social Security number). Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

If you find items you don't understand on your report, call the credit bureaus at the number given on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

**Contact the U.S. Federal Trade Commission.** If you detect any unauthorized transactions in your financial account, promptly notify your financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission. If you believe your identity has been stolen, the U.S. 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](http://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.

You can learn more about how to protect yourself from becoming a victim of identity theft by contacting the FTC:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
[www.ftc.gov/idtheft/](http://www.ftc.gov/idtheft/)

**Place a Fraud Alert on Your Credit File.** To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity

theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790	800-680-7289	www.transunion.com

**Place a Security Freeze on Your Credit File.** You may wish to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze by contacting each of the three credit bureaus at:

Equifax	P.O. Box 105788 Atlanta, Georgia 30348	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790	www.transunion.com

The credit bureaus may charge a reasonable fee to place a freeze on your account and may require that you provide proper identification prior to honoring your request.

**For Maryland Residents.** You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at:

Maryland Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
888-743-0023  
www.oag.state.md.us