



Hewlett-Packard Company
200 Forest Street
Mail Stop MRO1-3/CS
Marlborough, MA 01752
www.hp.com

Paul Henrion
Privacy Counsel
Hewlett-Packard Company

508-467-4018 Tel
508-467-4022 Fax
paul.henrion@hp.com

December 4, 2008

Massachusetts Attorney General
Martha Coakley
McCormack Building
One Ashburton Place
Boston, MA 02108

Re: Data Security Incident

Dear Ms. Coakley:

In accordance with Mass. Gen. Laws ch. 93H (H.B. 4144), 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 2054 Massachusetts 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 affected individuals. If you have any questions, please do not hesitate to contact me.

Very truly yours,


Paul Henrion
Privacy Counsel
Hewlett-Packard

[Insert HP Letterhead]

[Notification to Massachusetts Residents]

[Insert date], 2008

[Name
Address]

Dear Participant:

I am writing to inform you of an incident involving certain personal information of some participants in the HP benefits program. The information included names and Social Security numbers of some current and former employees. This incident occurred several months ago and HP has been working closely with law enforcement authorities to resolve it. 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. We have no evidence indicating that any of the information has been accessed or misused. Nevertheless, we encourage you to remain vigilant 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 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 AlertSM 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 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 AlertSM credit monitoring product at no cost to you. Triple AlertSM will be provided by ConsumerInfo.com, Inc. an Experian[®] company and will monitor your credit reports at the three national credit reporting companies: Experian, Equifax[®] and TransUnion[®] and notify you of key changes. Triple AlertSM is a powerful tool that will help you identify potentially fraudulent use of your information. Your Triple AlertSM membership is completely free and will not hurt your credit score.

The complimentary 24-month Triple AlertSM 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

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]**

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 for Massachusetts Residents

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, 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 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) 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/

Obtain a Police Report. You have the right to obtain a police report if you are the victim of identity theft.

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 you a fee of up to \$5 to place a freeze on your account and may require that you provide proper identification prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you provide the credit bureaus with a valid police report. When requesting a security freeze with each of the credit bureaus, you will be required to provide the following information:

For Equifax. Your full name, current residential address, date of birth, Social Security number and proof of your current address (such as a current utility bill).

For Experian. Your full name, with middle initial and generation (such as Jr., Sr., II, III), Social Security number, date of birth, current address and previous address(es) for the past 2 years. You also will need to provide one copy of a government-issued identification card (such as a driver's license, state or military identification card) and one copy of a utility bill, bank or insurance statement, etc. Make sure that each copy is legible, displays your name and current mailing address and the date of issue. Please note that the statement dates must be recent.

For TransUnion. Your name, current residential address, Social Security number, credit card number and expiration date (to pay the \$5 fee). You also will need to provide proof of your current residence (such as a driver's license or state issued identification card).



Hewlett-Packard Company
200 Forest Street
Mail Stop MRO1-3/K8
Marlboro, MA 01752
www.hp.com

508-467-4018 Tel
508-467-4022 Fax

To
Martha Cookley

Company
Massachusetts Attorney General
McCormack Building
One Ashburton Place
Boston, Massachusetts 02108

Telephone
(617) 727-2200

Fax
(617) 727-5765
attn: Scott Schafer

From
Paul Henrion

Subject
Data Security Incident

Number of Pages
6 including cover sheet

Date
December 4, 2008

CONFIDENTIALITY NOTICE: Unless otherwise indicated or obvious from the nature of this transmittal, the information contained in this facsimile message may be privileged, HP confidential, or confidential information subject to a court order, and therefore is intended solely for the use of the recipient named above. If you are not the intended recipient, then any dissemination, distribution, or copying of this communication is strictly prohibited. If you received this transmission in error, please immediately notify the sender by telephone, at our expense.

** TX STATUS REPORT **

AS OF DEC 04 '08 15:49 PAGE.01

HP LEGAL LKG MA

	DATE	TIME	TO/FROM	MODE	MIN/SEC	PGS	CMD#	STATUS
25	12/04	15:47	916177275765	EC--S	01'57"	006		OK

Paul B. Hannon
Hewlett-Packard Company
200 Forest Street
MRO1-3K8
Marlborough, MA 01752



JCL51112602623

SHIP TO: (617) 727-2200 **BILL SENDER**

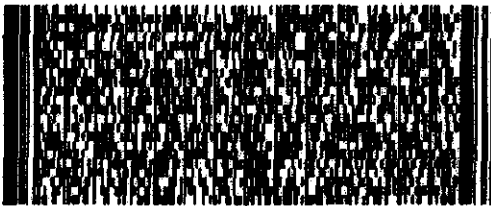
Marthy Coakley
Massachusetts Attorney General
McCormack Building
One Ashburton Place
Boston, MA 02108

ActWgt: 1.0 LB
CAD: 1007396/NET8091
Account#: S *****

Delivery Address Bar Code



Ref #
Invoice #
PO #
Dept #

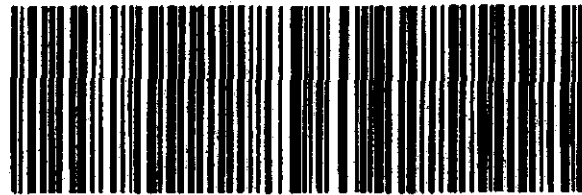


TRK# 7971 5645 2120
0201

FRI - 05DEC A
PRIORITY OVERNIGHT

01 LWMA

02108
MA-US
BOS



After printing this label:

1. Use the 'Print' button on this page to print your label to your laser or inkjet printer.
2. Fold the printed page along the horizontal line.
3. Place label in shipping pouch and affix it to your shipment so that the barcode portion of the label can be read and scanned.

Warning: Use only the printed original label for shipping. Using a photocopy of this label for shipping purposes is fraudulent and could result in additional billing charges along with the cancellation of your FedEx account number.

Use of this system constitutes your agreement to the service conditions in the current FedEx Service Guide, available on fedex.com. FedEx will not be responsible for any claim in excess of \$100 per package, whether the result of loss, damage, delay, non-delivery, misdelivery or misinformation, unless you declare a higher value, pay an additional charge, document your actual loss and file a timely claim. Limitations found in the current FedEx Service Guide apply. Your right to recover from FedEx for any loss, including intrinsic value of the package, loss of sale, income interest, profit, attorney's fees, costs, and other forms of damage whether direct, incidental, consequential, or special is limited to the greater of \$100 or the authorized declared value. Recovery cannot exceed actual documented loss. Maximum for items of extraordinary value is \$500, e.g. jewelry, precious metals, negotiable instruments and other items listed in our Service Guide. Written claims must be filed within strict time limits, see current FedEx Service Guide.

Global Home | FedEx Mobile | Service Info | About FedEx | Investor Relations | Careers | fedex.com Terms of Use | Privacy Policy | Site Map
This site is protected by copyright and trademark laws under US and International law. All rights reserved. © 1995-2008 FedEx

JAN 16 2009
EXPRESS
PROCESSED



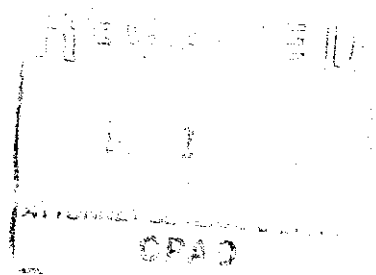
Hewlett-Packard Company
200 Forest Street
Mail Stop MRO1-3/CS
Marlborough, MA 01752
www.hp.com

Paul Henrion
Privacy Counsel
Hewlett-Packard Company

508-467-4018 Tel
508-467-4022 Fax
paul.henrion@hp.com

December 11, 2008

Shannon Choy-Seymour
Assistant Attorney General
Consumer Protection Division
Office of the Attorney General
Commonwealth of Massachusetts
One Ashburton Place
Boston, Massachusetts 02108



Dear Ms. Choy-Seymour:

Thank for your letter of December 8, 2008 inquiring pursuant to G.L. c. 93H § 3 as to any steps taken or planned to be taken relating to the incident to help ensure that this type of incident does not happen in the future.

Based on the review completed to date, HP is taking the following steps:

- Reports of lost or stolen laptops and other mobile devices with data storage will be directed initially to IT Security rather than the physical security organization regardless of which security organization initially receives the report;
- The initial list of questions that all employees will be asked is being expanded to provide clearer examples and descriptions of the potential sensitive data;
- Additionally, if the lost or stolen report is received from an employee in a high risk position with regular access to and processing of sensitive data, the backup files on the individual's impacted system will be checked regardless of the employee's response;
- Broad based communications about the new reporting process and the need for it will be made to employees company wide;
- Additional targeted training to HR professionals about the new process and proper sensitive data handling will be conducted; and
- Additional targeted training to Security, Privacy and Legal employees who may receive incident reports will be conducted.

If you have any questions, please do not hesitate to contact me.

Very truly yours,

Paul Henrion
Privacy Counsel
Hewlett-Packard



Hewlett-Packard Company
200 Forest Street
Mail Stop MRO1-3/C5
Marlborough, MA 01752
www.hp.com

Paul Henion
Privacy Counsel
Hewlett-Packard Company

508-467-4018 Tel
508-467-4022 Fax
paul.henion@hp.com

January 15, 2009

Massachusetts Attorney General
Martha Coakley
McCormack Building
One Ashburton Place
Boston, MA 02108

Re: Data Security Incident

Dear Ms. Coakley:

In accordance with Mass. Gen. Laws ch. 93H (H.B. 4144), 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 4, 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. The bank account number of one Massachusetts resident without password was also on the laptop. We are working with law enforcement authorities to recover the stolen laptop. At this time, we are aware of approximately 2985 Massachusetts residents who may be affected by this incident beyond the 2054 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.

Very truly yours,


Paul Henion
Privacy Counsel
Hewlett-Packard



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 an incident involving certain personal information of some participants in the HP benefits program. The information included names, Social Security numbers, medical history, diagnosis or treatment, and health insurance account numbers of some current and former employees. This incident occurred several months ago and HP has been working closely with law enforcement authorities to resolve it. 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. We have no evidence indicating that any of the information has been accessed or misused. Nevertheless, we encourage you to remain vigilant 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 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 AlertSM 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 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 AlertSM credit monitoring product at no cost to you. Triple AlertSM will be provided by ConsumerInfo.com, Inc. an Experian[®] company and will monitor your credit reports at the three national credit reporting companies: Experian, Equifax[®] and TransUnion[®] and notify you of key changes. Triple AlertSM is a powerful tool that will help you identify potentially fraudulent use of your information. Your Triple AlertSM membership is completely free and will not hurt your credit score.

The complimentary 24-month Triple AlertSM 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

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 for Massachusetts Residents

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, 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 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) 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/

Obtain a Police Report. You have the right to obtain a police report if you are the victim of identity theft.

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 you a fee of up to \$5 to place a freeze on your account and may require that you provide proper identification prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you provide the credit bureaus with a valid police report. When requesting a security freeze with each of the credit bureaus, you will be required to provide the following information:

For Equifax. Your full name, current residential address, date of birth, Social Security number and proof of your current address (such as a current utility bill).

For Experian. Your full name, with middle initial and generation (such as Jr., Sr., II, III), Social Security number, date of birth, current address and previous address(es) for the past 2 years. You also will need to provide one copy of a government-issued identification card (such as a driver’s license, state or military identification card) and one copy of a utility bill, bank or insurance statement, etc. Make sure that each copy is legible, displays your name and current mailing address and the date of issue. Please note that the statement dates must be recent.

For TransUnion. Your name, current residential address, Social Security number, credit card number and expiration date (to pay the \$5 fee). You also will need to provide proof of your current residence (such as a driver’s license or state issued identification card).



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

January X, 2009

[Name]
[Address]
[Address]

Dear Participant:

I am writing to update you on an incident involving certain personal information of some participants in the HP benefits program. You were previously mailed a notice concerning this incident earlier in December. In addition to the previously notified 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 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