



March, 21, 2006

Dear Participants in Hewlett-Packard sponsored Retirement Plans (including current and former Hewlett-Packard employees, as well as former employees of acquired companies):

Please Read This Important Notice

We are writing to let you know that a laptop computer containing personally identifiable information used for a business meeting was recently stolen. We believe that identifying information about you was contained in the laptop.

Law enforcement was notified after we learned of the theft and is conducting an investigation.

At this time, we are not aware that the information contained in the laptop has been misused. Even so, we want to inform you of the situation and to suggest some steps you can take to protect yourself from identity theft now and in the future.

We deeply regret this situation and are keenly aware of how important your personal information is to you. This letter is to provide you with information you need to understand the situation and to protect yourself from misuse of your information, including identity theft.

What happened?

A laptop belonging to Fidelity Investments, which provides services to the Participants in Hewlett-Packard sponsored Retirement Plans (including current and former Hewlett-Packard employees, as well as former employees of acquired companies) ("HP Participants"), was stolen on the evening of March 15th.

The laptop contained personal data of HP Participants, including names, Social Security numbers, addresses, dates of birth, compensation, and other employee retirement plan information. It is important for you to know that the license to the software which contained the data has expired. As a result, the scrambled data is difficult to interpret. We have no evidence that the information has been misused. Further, it is in a form that is generally unusable.

What steps has Fidelity taken?

We have alerted our Fidelity representatives to this situation and implemented extra security processes requiring additional authentication for access to your account as well as other measures to prevent unauthorized use. Accordingly, we encourage you to be prepared to provide additional personal and/or account information to verify your identity.

We also have employed additional security controls above and beyond our already significant monitoring activity to identify if there is any unusual activity in your Fidelity accounts.

We are contacting the three principal credit reporting bureaus, Equifax, Experian, and TransUnion, to advise them of the situation.

Fidelity 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, although we have no knowledge of any misuse of this information. The service is provided by Equifax, one of the major credit reporting companies that monitors activity.

To enroll in the Equifax Credit Watch™ service, simply fill out the enclosed form and return it to Equifax. Or, enroll online at www.myservices.equifax.com/monitor_order and use the promotional code from the attached directions. Once you have enrolled, you will be provided with several valuable services including credit monitoring, a copy of your credit report, notification of activity, additional access to your credit report, and some level of identity theft insurance for expenses. In addition, you will have access 24 hours a day, 7 days a week to Equifax's customer service representatives.

What additional actions can you take to protect yourself?

It is always a good practice to regularly review activity on your accounts and to obtain your credit report from one or more of the national credit reporting companies. We recommend that you remain vigilant for at least the next 12 to 24 months, and to promptly report any incidents of suspected identity theft to us and to the proper authorities.

The enclosed Reference Guide will provide you more information on identify theft, how to report it and how to protect yourself.

Please know that Fidelity is treating this matter extremely seriously. We value your business and the trust you have placed in Fidelity and we deeply regret any inconvenience or concerns this may cause you.

If you have any questions or need additional information, our representatives are prepared to help you. Please call 1-800-414-4015.

Sincerely,



William G. Duserick
Vice President, Chief Privacy Officer
Fidelity Investments

We also have employed additional security controls above and beyond our already significant monitoring activity to identify if there is any unusual activity in your Fidelity accounts.

We are contacting the three principal credit reporting bureaus, Equifax, Experian and Trans Union, to advise them of the situation.

Fidelity 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, although we have no knowledge of any misuse of this information. The service is provided by Equifax, one of the major credit reporting companies that monitors activity. For details on how to enroll in this service, log on to Fidelity NetBenefits® at <https://netbenefits.fidelity.com>. From the NetBenefits home page, click on the link in the News section on the right hand side of the home page. Once you have enrolled, you will be provided with several valuable services including credit monitoring, a copy of your credit report, notification of activity, additional access to your credit report, and some level of identity theft insurance for expenses. In addition, you will have access 24 hours a day, 7 days a week to Equifax's customer service representatives.

What additional actions can you take to protect yourself?

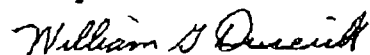
It is always a good practice to regularly review activity on your accounts and to obtain your credit report from one or more of the national credit reporting companies. We recommend that you remain vigilant for at least the next 12 to 24 months, and to promptly report any incidents of suspected identity theft to us and to the proper authorities.

The enclosed Reference Guide will provide you more information on identify theft, how to report it and how to protect yourself.

Please know that Fidelity is treating this matter extremely seriously. We value your business and the trust you have placed in Fidelity and we deeply regret any inconvenience or concerns this may cause you.

If you have any questions or need additional information, our representatives are prepared to help you. Please call 1-800-414-4015.

Sincerely,



William G. Duserick
Vice President, Chief Privacy Officer
Fidelity Investments



FAX

- Fidelity Internal Information
- Fidelity Confidential Information
- Fidelity Highly Confidential Information

To: CONSUMER PROTECTION BOARD
 Company: NEW YORK STATE
 Phone: _____
 Fax: 518 474 2474

From: WILLIAM DUSERICK
 Phone: 617 392 1224
 Fax: 617 476 6578
 cc: _____
 Date: March 21, 2006

Pages inc. cover: 8

Caution: The message and any documents accompanying this transmission (the "transmission") contain information from FMR Corp. or its affiliates that is proprietary, confidential, and/or subject to the attorney-client privilege. The transmission is intended only for the person specifically named above. If you are not the intended recipient of this information, or the employee/agent responsible for delivering this message, you are hereby notified that any dissemination, distribution, or copying of this information is strictly prohibited. If you have received this message in error, please notify us immediately by telephone (call us collect if you wish) and return the original to us at the address below, at our cost.

Comments:

REFERENCE GUIDE

While there is no indication that the data on the laptop has been misused, it is prudent to know about identity theft and what you can do to protect yourself.

About Identity Theft

Identity theft, in its simplest form, occurs when someone obtains and misuses your personal information without your permission, and often times without your knowledge of the activity.

Identity Theft Prevention

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 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.

In addition, under federal law you are entitled to a free copy of your credit report, at your request, from each of the major nationwide credit reporting companies once every 12 months. 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. Please do not contact the three nationwide credit reporting companies individually. If you ask, only the last four digits of your Social Security number will appear on your credit reports.

To learn more about how to protect yourself against identity theft, please visit www.consumer.gov/idtheft or call the Federal Trade Commission hotline phone number: 1-877-IDTHEFT (438-4338). You may call or visit the Federal Trade Commission Web site to report any incident of suspected identity theft.

REFERENCE GUIDE

While there is no indication that the data on the laptop has been misused, it is prudent to know about identity theft and what you can do to protect yourself.

About Identity Theft

Identity theft, in its simplest form, occurs when someone obtains and misuses your personal information without your permission, and often times without your knowledge of the activity.

Identity Theft Prevention

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 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.

In addition, under federal law you are entitled to a free copy of your credit report, at your request, from each of the major nationwide credit reporting companies once every 12 months. 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. Please do not contact the three nationwide credit reporting companies individually. If you ask, only the last four digits of your Social Security number will appear on your credit reports.

To learn more about how to protect yourself against identity theft, please visit www.consumer.gov/idtheft or call the Federal Trade Commission hotline phone number: 1-877-IDTHEFT (438-4338). You may call or visit the Federal Trade Commission Web site to report any incident of suspected identity theft.



March, 21, 2006

Dear Participants in Hewlett-Packard sponsored Retirement Plans:

Please Read This Important Notice re: Security Alert

We are writing to let you know that a laptop computer containing personally identifiable information used for a business meeting was recently stolen. We believe that identifying information about you was contained in the laptop.

Law enforcement was notified after we learned of the theft and is conducting an investigation.

At this time, we are not aware that the information contained in the laptop has been misused. Even so, we want to inform you of the situation and to suggest some steps you can take to protect yourself from identity theft now and in the future.

We deeply regret this situation and are keenly aware of how important your personal information is to you. This letter is to provide you with information you need to understand the situation and to protect yourself from misuse of your information, including identity theft.

What happened?

A laptop belonging to Fidelity Investments, which provides services to the Participants in Hewlett-Packard sponsored Retirement Plans (including current and former Hewlett-Packard employees, as well as former employees of acquired companies) ("HP Participants"), was stolen on the evening of March 15th.

The laptop contained personal data of HP Participants, including names, Social Security numbers, addresses, dates of birth, compensation and other employee retirement plan information. *It is important for you to know that the license to the software which contained the data has expired. As a result, the scrambled data is difficult to interpret. We have no evidence that the information has been misused. Further, it is in a form that is generally unusable.*

What steps has Fidelity taken?

We have alerted our Fidelity representatives to this situation and implemented extra security processes requiring additional authentication for access to your account as well as other measures to prevent unauthorized use. Accordingly, we encourage you to be prepared to provide additional personal and/or account information to verify your identity.

**Reporting Form
For Business, Individual or NY State Entity reporting a
"Breach of the Security of the System"
Pursuant to the Information Security Breach
and Notification Act (General Business Law §889-aa;
State Technology Law §208)**

Name of Business, Individual or State Entity: Fidelity Investments
 Date of Discovery of Breach: on or about March 15, 2006
 Estimated Number of Affected Individuals: approx. 2800 NY residents (total approx. 196,000)
 Date of Notification to Affected Individuals: March 21-22, 2006
 Manner of Notification: written notice
 electronic notice (email)
 telephone notice

Are you requesting substitute notice? Yes No (If yes, attach justification)

Content of Notification to Affected Individuals: Describe what happened in general terms and what kind of information was involved. Please attach copy of Notice.

A Fidelity-owned laptop computer was stolen in California. The laptop contained personal data of retirement plan participants including names, addresses, Social Security numbers, dates of birth, compensation and other employment information. The license on the software used to access the data has expired making the data difficult to interpret. We are not aware of misuse of this data, but have implemented additional security measures to prevent unauthorized use of this data and account access.

Law enforcement has been notified as well as the national credit bureaus, Equifax, Experian and TransUnion.

A copy of the notices to participants is attached.

Name of Business or Individual Contact Person: William Duserick
 Title: Vice President, Chief Privacy Officer
 Telephone number: 617-392-1224
 Email: William.Duserick@fmr.com

Dated: March 21, 2005
 Submitted by: William Duserick
 Title: Vice President, Chief Privacy Officer
 Address: 82 Devonshire Street, Mail Zone ZW10B, Boston, MA 02109
 Email: William.Duserick@fmr.com