



March 21, 2006

Attorney General Roy Cooper
Consumer Protection Division
North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, North Carolina 27699-9001

Re: Notice of Potential Information Security Breach Pursuant to N.C. Gen. Stat. § 75-65


Dear Attorney General Cooper:

In accordance with N.C. Gen. Stat. § 75-65, we write to inform you of a possible information security breach regarding individuals we service that occurred on or about March 15, 2006. We estimate that approximately 196,000 individuals may have been affected by this incident. Pursuant to our obligations under N.C. Gen. Stat. § 75-65, commencing today we are sending notification by overnight mail to all affected individuals residing in North Carolina and elsewhere of the information security breach. In addition, because this incident potentially involved more than 1,000 North Carolina residents, we notified consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the incident on March 21, 2006.

The notices describe (1) the general nature of the incident resulting in the potential information security breach, (2) the type of personal information that was the subject of the possible security breach, (3) the precautionary measures we are taking to help protect affected individuals from unauthorized access, (4) contact information for inquiries regarding the incident, (5) a guide for affected individuals to protect against and respond to identity theft and/or misuse of their personal information, and (6) advice to affected individuals that they remain vigilant by reviewing account statements and monitoring free credit reports that are available to them.

For your convenience, a copy of the notices sent to affected individuals in North Carolina and elsewhere is enclosed with this letter. If you have any questions or need further information regarding this incident, please do not hesitate to contact us.

Sincerely yours,


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

Enclosures



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.

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

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 (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

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.



Margaret H. Raymond
 Vice President and
 Assistant General Counsel

April 19, 2006

BY TELECOPIER (919) 716-6050

CONFIDENTIAL TREATMENT REQUESTED
 UNDER NORTH CAROLINA F.O.I.A.

Joshua H. Stein
 Senior Deputy Attorney General
 State of North Carolina
 Department of Justice-Consumer Protection
 9001 Mall Service Center
 Raleigh, NC 27699-9001

Re: Security Breach Notification

Dear Mr. Stein:

I write to respond to the questions posed in your letter dated March 27, 2006 to William Duserick, Chief Privacy Officer for Fidelity Investments. Fidelity Investments is a trade name commonly used for a group of companies owned by FMR Corp.

Approximately 1,521 individuals residing in North Carolina were impacted by the incident.

The stolen laptop was password-protected. During the business presentation at which the laptop and the associated retirement plan data were used, the password was attached to a Post-It note on the outside of the laptop computer. It is unclear whether the note remained on the laptop at the time of the theft.

The data on the laptop was not technically encrypted. The data had been loaded onto the laptop in order to demonstrate to Hewlett Packard Company ("HP") representatives a third-party actuarial software product. The pension actuarial software was intended to answer HP's concerns that our proprietary reporting tool for the HP plans was cumbersome and inadequate for retirement plans with data as complex as that of the HP plans. In order to provide a robust demonstration with real world data, actual HP plan data was loaded onto the laptop, in the form of a database, along with a copy of the third party actuarial software under a temporary license. The temporary license (known



Joshua Stein, Esq.
 April 19, 2006
 Page 2

as a "commuter key") expired on the morning of March 17, 2006, approximately 36 hours after the theft. After expiration of the software license, the data was generally unusable, in the sense that data elements associated with each other in the database had no readily apparent relationship with each other in the absence of the software. In addition, number strings were stored in binary format, and were not generally understandable as particular numeric portions of personally identifiable information (e.g., social security numbers or dates of birth). The information was not, however, encrypted.

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

* * * * *

This letter is being provided to the North Carolina Office of the Attorney General as part of that office's investigation of events surrounding this matter. Accordingly, this letter is entitled to exemption from public disclosure under the Freedom of Information Act, North Carolina's governing statute, N.C.G.S. c. 132-1, and other applicable provisions of law governing the non-disclosure of information. The letter contains proprietary information. In addition, the disclosure of this letter could put the firm at a competitive disadvantage. This letter is being provided with the further understanding that: (i) you will keep it strictly confidential and will not disclose or provide it to any other party, unless (a) you determine that disclosure should be made to another government agency or self-regulatory organization ("SRO"), in which case you will notify the undersigned prior to initiating such disclosure and will use your best efforts to obtain confirmation from the government agency or SRO that the letter will be accorded confidential treatment; or (b) you receive a subpoena or other compulsory order seeking production of the letter, in which case you will notify the undersigned immediately and provide us an opportunity to prove that the letter qualifies for an exemption from public disclosure; and (ii) the letter does not constitute any authorization, consent or waiver by FMR Corp. or its affiliates or subsidiaries, express or implied, entitling the North Carolina Office of the Attorney General or any other agency or person to have access to any additional documents or information in the possession of FMR Corp. or its affiliates or subsidiaries. Finally, we request that this letter be returned to the undersigned upon the completion of your inquiry.

Sincerely yours,

Margaret H. Raymond
 Vice President, Associate General Counsel

cc: David C. Boch, Esq.