



SIDLEY AUSTIN LLP
 1501 K STREET, N.W.
 WASHINGTON, D.C. 20005
 (202) 736 8000
 (202) 736 8711 FAX

BEIJING GENEVA SAN FRANCISCO
 BRUSSELS HONG KONG SHANGHAI
 CHICAGO LONDON SINGAPORE
 DALLAS LOS ANGELES TOKYO
 FRANKFURT NEW YORK WASHINGTON, DC
 FOUNDED 1866

FACSIMILE/TELECOPIER TRANSMISSION

From: Name: Edward R. McNicholas
 Voice: (202) 736-8010

To: Name: CPB Security Breach Notification
 Company:
 Facsimile#: 518-474-2474
 Voice Phone:
 Subject:

Date: 8/9/2006 **Time:** 4:50:07 PM **No. Pages (Including Cover):** 4

Message:

IRS CIRCULAR 230 DISCLOSURE: To comply with certain U.S. Treasury regulations, we inform you that, unless expressly stated otherwise, any U.S. federal tax advice contained in this communication, including attachments, was not intended or written to be used, and cannot be used, by any taxpayer for the purpose of avoiding any penalties that may be imposed on such taxpayer by the Internal Revenue Service. In addition, if any such tax advice is used or referred to by other parties in promoting, marketing or recommending any partnership or other entity, investment plan or arrangement, then (i) the advice should be construed as written in connection with the promotion or marketing by others of the transaction(s) or matter(s) addressed in this communication and (ii) the taxpayer should seek advice based on the taxpayer's particular circumstances from an independent tax advisor.

Problems with this transmission should be reported to:

THIS MESSAGE IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL(S) OR ENTITY(IES) TO WHICH IT IS ADDRESSED AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL AND EXEMPT FROM DISCLOSURE UNDER APPLICABLE LAW. IF THE READER OF THIS MESSAGE IS NOT THE INTENDED RECIPIENT OR THE EMPLOYEE OR AGENT RESPONSIBLE FOR DELIVERING THE MESSAGE TO THE INTENDED RECIPIENT, YOU ARE HEREBY NOTIFIED THAT ANY DISSEMINATION, DISTRIBUTION OR COPYING OF THIS COMMUNICATION IS STRICTLY PROHIBITED. IF YOU HAVE RECEIVED THIS COMMUNICATION IN ERROR, NOTIFY US IMMEDIATELY BY TELEPHONE AND RETURN THE ORIGINAL MESSAGE TO US AT THE ABOVE ADDRESS VIA THE U.S. POSTAL SERVICE.

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 §209)

Name of Business, Individual or State Entity Hoffmann-La Roche Inc.
Date of Discovery of Breach: July 18, 2006 by McGladrey & Pullen LLP
Estimated Number of Affected Individuals: 1500 New York residents
Date of Notification to Affected Individuals: August 9, 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 laptop computer belonging to McGladrey & Pullen LLP, the independent third-party auditing firm hired to conduct a legally-required annual audit of the Roche Savings and Pay Deferral Plan, was stolen on July 18, 2006, from one of the auditor's employees. The laptop included Plan-related information including names, Social Security numbers, affiliation with the Plan, Plan account balance, and 2005 Plan withdrawal amounts, if any.

Name of Business or Individual Contact Person: Edward R. McNicholas (outside counsel)
Title: Partner, Sidley Austin LLP
Telephone number: (202) 736-8010
Email: emcnicholas@sidley.com

Dated: August 9, 2006
Submitted by: Edward R. McNicholas
Title: Partner, Sidley Austin LLP
Address: 1501 K Street NW, Washington, DC 20005
Email: emcnicholas@sidley.com
Telephone: (202) 736-8010 Fax: (202) 736-8711



PERSONAL AND CONFIDENTIAL

August 9, 2006

We are writing to you as a current or former participant, beneficiary, or alternate payee of the Roche Savings and Pay Deferral Plan (the "Plan") in our capacity as the Plan's record keeper. Hoffmann-La Roche Inc. ("Roche"), the Plan Sponsor, has asked us to inform you of the following information:

A laptop computer belonging to the independent third-party auditing firm hired by the Plan Sponsor to conduct a legally-required annual audit was stolen on July 18, 2006, from one of the auditor's employees. The laptop contained Plan-related information, including your name, Social Security number, your affiliation with the Plan, Plan account balance, and 2005 Plan withdrawal amounts, if any. On August 7, 2006, the auditing firm established certain pertinent facts surrounding the theft. We have been told by the third party auditing firm that, through their investigation to date, they have no reason to believe that any other Plan-related information has been compromised. The auditing firm has given assurances that the stolen computer had security measures in place, including two layers of password protection. To date, there has been no indication that any Plan-related information on the laptop has been accessed or misused. The auditors notified law enforcement officials of the laptop theft and an investigation is underway.

As a precaution, after discussions with Roche, Fidelity began actively monitoring the Plan accounts to try to detect any suspicious activity. Our review to date has not shown any indication of unauthorized activity.

It is important to note that there are safeguards in place to protect your Plan account from unauthorized activity. For example, if you have set up online access to your Plan account, the account is protected by requiring a Personal Identification Number ("PIN") to gain online access. Beyond the normal security regularly in place on Plan accounts, we have implemented heightened monitoring procedures for these accounts to try to identify potential unauthorized activity.

While we are taking extra precautions, you may wish to take some or all of the following steps to protect further against the potential misuse of your personal and Plan account data, if applicable, and as a matter of prudent financial account management:

1. Change your Fidelity Customer ID and your account PIN by logging onto NetBenefits at www.401k.com, or calling 1-800-269-4015. Although there are safeguards in place to protect your account, and while we have no reason to believe that your PIN has been compromised, it is good practice to change your PIN regularly. If your Social Security number currently serves as the Customer ID for your account, you should consider changing it to a different identifier. Please note that if you have other accounts where your Social Security number is used as an identifier, you may wish to change the identifier and/or PIN for those accounts as well.

2. Place a fraud alert or freeze on your credit report. A fraud alert is designed to prevent credit, loans, and services from being approved in your name without your consent. This provides an enhanced level of protection; however, it may limit your ability to get immediate credit, including offers available at retail stores. A fraud alert is effective for 90 days and may be renewed. You must contact at least one of the credit reporting agencies directly to request this alert. See the enclosed list for names, addresses, and phone numbers for the three national credit reporting agencies. Some states allow their residents to place freezes on their credit reports. Freezes prevent the sharing of credit report information to most third parties; however, some fees may apply to place a freeze or lift a freeze. Should you be interested, please contact one of the credit reporting agencies for details about placing a freeze.

PERSONAL AND CONFIDENTIAL

3. Review account activity often for at least the next 12 months. Promptly report any suspicious activity, including transactions you do not recognize, to the appropriate financial institution. For example, contact Fidelity if you suspect there is suspicious activity pertaining to your Plan account or other accounts with Fidelity.

4. Order and review your credit report immediately and continue to do so over the course of the next year, to check for fraudulent or other unusual activity. You may order your credit report from any one of the agencies listed below. Additionally,

- You can order a free annual credit report by calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.
- When you receive a credit report, check it carefully. In particular, check for any accounts that you may not have opened and any inquiries from creditors that you did not initiate. Verify your personal information, including address and Social Security number, on the reports. If you see anything incorrect or that you do not understand, contact the credit agency immediately.
- If you find suspicious activity on your credit report, contact your local police or sheriff's office to file a police report regarding identity theft. Maintain a copy of the police report; you may need to provide copies of the report to creditors to clear your records. You can also contact the Federal Trade Commission's Identity Theft Hotline at 1-877-438-4338 if you suspect someone has misappropriated your personal information.

For more information on identity theft and on how to protect yourself from fraud, you may visit the Federal Trade Commission's special website dedicated to these topics at www.consumer.gov/idtheft.

If you have any questions, or if we may be of any further assistance to you, please call us at 800-269-4015. This is a toll-free number dedicated to Roche Plan participants. Team members will be available 8:30 a.m. to 12:00 midnight Eastern time to address your questions or concerns.

Credit Reporting Agencies

TransUnion
Fraud Victim Assistance Dept.
P.O. Box 6790
Fullerton, CA 92634
1-800-680-7289

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-525-6285

Experian
P.O. Box 9530
Allen, TX 75013
1-888-397-3742

Sincerely,

Fidelity Investments