

DICKSTEINSHAPIRO_{LLP}

1825 Eye Street NW | Washington, DC 20006-5403
TEL (202) 420-2200 | FAX (202) 420-2201 | dicksteinshapiro.com

March 19, 2008

Honorable Martha Coakley
Attorney General of Massachusetts
One Ashburton Place
Boston, MA 02108

Re: Recent Laptop Theft

Dear General Coakley:

I am writing to give you notice of a recent data security incident involving an independent contractor working for my client, Pfizer Inc ("Pfizer"). On February 7, 2008, the home of the contractor, who assists in arranging and planning travel and meetings for Pfizer, was burglarized and the contractor's laptop computer was stolen. Some information about present and former Pfizer employees and individuals providing contract services to Pfizer was stored on that laptop.

The police were notified immediately, but no arrests have been made, and the laptop has not been recovered. Pfizer has been working with the contractor to assess the information contained on the stolen laptop. The contractor maintained an external back-up hard drive of the laptop's contents, and from the initial examination of the back-up it appears that the laptop contained information about approximately 800 individuals, including approximately 15 residents of your state. The forensic review to date indicates that the information included names and credit card numbers, as well as, in some instances, credit card expiration dates, home and/or business addresses, home and/or business and/or cell phone numbers, personal and/or business e-mail addresses, hotel loyalty program numbers and other travel and logistics information. The forensic review is ongoing, but it does not appear that any passwords or PIN codes for the credit cards were exposed, nor were any Social Security numbers exposed.

The laptop was password protected. At this time Pfizer is not aware that any person has inappropriately used any exposed information, but the Company is continuing to monitor the situation.

Pfizer is planning to send notification letters to all affected individuals within the next few days to inform them about the data loss and provide information about the types of data exposed, as described above. Pfizer has also notified the three major national credit reporting agencies about the incident. In addition, Pfizer has arranged to provide all affected individuals with the opportunity to sign-up for a full 2-year package of credit-protection services and identity theft insurance, free of charge.

Events of this nature are unfortunate and difficult to avoid, and Pfizer is grateful that nobody was injured during the robbery. Pfizer continues its ongoing efforts to enhance and improve data

DICKSTEINSHAPIRO^{LLP}

Honorable Martha Coakley

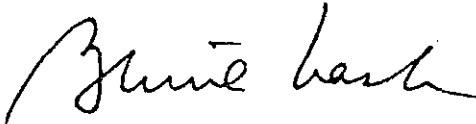
March 19, 2008

Page 2

security and privacy protections, including requirements for contractor laptop security and limits on the sensitive data that contractors can store, to reduce the risk of exposure of data on laptops.

I have attached a draft copy of the notification letter that is being sent to affected individuals in your state. Please do not hesitate to contact me if I can provide you with any additional information.

Very truly yours,

A handwritten signature in cursive script, appearing to read "Bernard Nash".

Bernard Nash

(202) 420-2209

nashb@dicksteinshapiro.com

Enclosure

Sample Name
Sample Address
Sample City, State, Zip Code

Dear [_____]:

We are writing to let you know that unfortunately, a security breach has exposed some of your personal information, including your name and credit card number, to unauthorized individuals. We are not aware of incidents of fraud or identity theft resulting from this data loss. However, you may wish to be alert for possible misuse of your personal information and we would like to offer you an opportunity to take advantage of support services that Pfizer is making available to help protect you

Pfizer deeply regrets this incident and any concerns it may raise. We hope that this letter, and the assistance that we are offering, will answer your questions and provide practical support.

What Information Was Exposed

Our analysis is ongoing, but presently, it appears that in addition to your name and a credit card number, some or all of the following information may have been exposed:

- *Credit card expiration date (month and year)
- *Office, Home and/or Cellular Telephone Number
- *Hotel Loyalty Program Account Number
- *Office and/or Home Address
- *Office and/or Home E-mail Addresses

Based on the analysis to date, Social Security numbers, credit card PIN numbers or passwords do not appear to have been exposed

What Pfizer Is Doing to Help Protect Your Privacy and Security

Pfizer has notified the three major U.S. credit bureaus, your state Attorney General, and other officials where required by law.

Pfizer also has retained Identity Safeguards ("IDS"), a specialist in credit security and identity theft protection, to offer you two years of credit protection and restoration services at Pfizer's expense, including:

- **Credit Monitoring:** IDS will provide credit monitoring that gives you unlimited access to your TransUnion credit report and score and will notify you of key changes in your TransUnion credit report.
- **Routine Updates:** You will receive ongoing email or SMS Text alerts about key changes to your credit reports from all three major credit agencies. Even if your credit reports do not change, you will be updated monthly or weekly (as you choose).
- **Fraud Resolution Representatives:** IDS will provide expert guidance if you suspect that your personal information is being misused.
- **Insurance Reimbursement:** IDS will arrange \$50,000 of Identity Theft insurance from a designated third party insurer.

More Strategies to Help Guard Your Credit and Identity

- Monitor your account statements and credit reports for unusual activity.
- Place a "fraud alert" on your credit file so that creditors are told to contact you before opening or changing an account. Since your Social Security number does not appear to have been exposed, a

fraud alert may not be as useful as in other situations. If you would like one anyway, the service is free and easy to request; when one major credit agency places an alert, it notifies the others to do so, too. Please note: you will be asked for your Social Security number. In general, in other circumstances, you should not give that number out.

Credit Agency	Fraud Alert Toll-Free No.	Website
Equifax	1-888-766-0008	www.equifax.com
Experian	1-888-397-3742	www.experian.com
TransUnion	1-800-680-7289	www.transunion.com

- Request a free credit report annually from each major credit agency. Checking your free credit report helps reduce risk from new accounts and may provide early notice of a potential fraud or incident of identity theft. To order, visit www.annualcreditreport.com or call toll-free **(877) 322-8228**.
- Call the credit agency if you do not understand something on your credit report. If you find suspicious activity on your credit report, call your local police or sheriff's office and file a report of identify theft. You have a right to a copy of the police report, and you should keep a copy because you may need it for creditors and it will be helpful if you decide to request a security freeze on your accounts, as described below. You also should file a complaint with the Federal Trade Commission ("FTC") at www.ftc.gov/idtheft or at 1-877-ID-THEFT (1-877-438-4338).
- Check your credit reports regularly. Identity thieves may hold personal information for a time before using it. Periodic checking can help you spot problems and address them quickly.
- You have a right to place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. However, placing a security freeze on your credit report may delay, interfere with, or prevent timely approval of requests you make for new loans, credit, mortgages, employment, housing or other services.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, the credit reporting agency cannot charge you to place, temporarily lift or remove a security freeze. In all other cases, a credit reporting agency may charge up to \$5 each to place, temporarily lift or remove a security freeze.

Each agency has slightly different requirements to place a security freeze.

Equifax

Send a written request, via certified mail, to Equifax Security Freeze, P.O. Box 105788, Atlanta, Georgia 30348, including the following information: name, address, date of birth, Social Security number, proof of current address, and payment, if appropriate. If you are an identity theft victim and are requesting a security freeze you will not be charged if you also include a copy of a police report, Identity Theft report, or other government law enforcement agency report, such as a DMV report.

Experian

Send a written request to Experian Security Freeze, P.O. Box 9554, Allen, TX 75013, including your full name, with middle initial and generation, such as JR, SR, II, III, etc.; Social Security number; date of birth (month, day and year); current address and previous addresses for the past two years; one copy of a government issued identification card, such as a driver's license, state or military ID card, etc., and one copy of a utility bill, bank or insurance statement, etc. Each copy must be legible and display your name and current mailing address, and the date of issue (statement dates must be recent). In addition, enclose payment, if appropriate, or, if you are a victim of Identity Theft and are

requesting a freeze without payment, enclose a valid investigative or incident report or complaint with a law enforcement agency or the DMV. You may also request a freeze via the internet at www.experian.com/freeze.

TransUnion

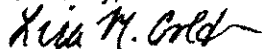
Submit a written request (you may make such a request by overnight mail) to TransUnion, Fraud Victim Assistance Department, P.O. Box 6790 Fullerton, CA 92834. Your request must include your name, address, Social Security number and a credit card number and expiration date to pay the applicable fee, if any, for the service. If you are a victim of identity theft and can provide TransUnion with a copy of a valid identity theft report, a department of motor vehicles investigation report, or similar proof that you have been a victim of identify theft, you will not be charged a fee for the Security Freeze services.

Remember, the IDS credit protection services package is free to you. The registration deadline is September 30, 2008. To register for the Pfizer-sponsored services, contact the Call Center at 866-910-5602, from Monday – Friday, 9 am – 9 pm (ET) or visit www.idsagu.com and enter the access code provided below, disregarding any pricing information.

Your Access Code: **[insert access code]**

Pfizer is serious about data security and protecting the privacy of personal information. We sincerely regret any inconvenience resulting from this unfortunate incident, and encourage you to take the opportunity to register for Pfizer-sponsored credit protection services to help protect your personal information. If you have questions, please send an email to privacy.officer@pfizer.com or call our Helpline at 212 733-0228.

Sincerely,



Chief Privacy Officer