

**North Carolina Security Breach Reporting Form  
Pursuant to the Identity Theft Protection Act of 2005**

Name of Business Owning or Licensing Information Affected by the Breach: Pfizer Inc  
Address: 235 East 42nd Street  
New York, NY 10017-5755  
Telephone: (212) 733-6640  
Fax: (646) 792-4565  
Email: Carlton.Wessel@pfizer.com

**PLEASE SUBMIT FORM TO:**  
Consumer Protection Division  
NC Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
Telephone: (919) 716-6000  
Toll Free in NC: (877) 566-7226  
FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: March 21, 2008  
Date the Security Breach was discovered: ~ February 11, 2008  
Estimated number of affected individuals: 800  
Estimated number of NC residents affected: 21

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b)): \_\_\_\_\_

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: Please see attached response

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. Please see attached response If so, please describe the security measures protecting the information: \_\_\_\_\_

Describe any measures taken to prevent a similar Security Breach from occurring in the future: Please see attached response

Date affected NC residents were/will be notified: March 20, 2008

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c): N/A

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified? (pursuant to N.C.G.S. § 75-65(e))  
Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

written notice  
 electronic notice (email)  
 telephone notice  
 substitute notice

Signature: *Pete Levitas* Date: March 21, 2008  
Contact Person, Title: Pete Levitas  
Address: Dickstein Shapiro LLP  
(if different from above) 1825 Eye Street, NW, Washington, DC 20006  
Telephone: (202) 420-3495 Fax: (202) 420-2201 Email: levitasp@dicksteinshapiro.com

**Addendum to North Carolina Security Breach Reporting Form**  
**Filed by Pfizer Inc**  
**March 21, 2008**

**Q. Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format:**

A. On February 7, 2008, the home of an independent contractor working for Pfizer, who assists in arranging and planning travel and meetings for Pfizer, was burglarized and the contractor's laptop 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.

The contractor maintained an external back-up hard drive of the laptop's contents, and the forensic review of that back-up to date indicates that the information exposed in electronic format 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.

**Q. Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. If so, please describe the security measures protecting the information:**

A. The information on the laptops was itself neither password protected nor encrypted. However, the laptop itself was password protected.

**Q: Describe any measures taken to prevent a similar Security Breach from occurring in the future:**

A. Pfizer is doing an extensive review of its policies and procedures to enhance and improve data security and privacy protections, including limits on the sensitive data that contractors can store and requirements for contractor laptop security, to reduce the risk of exposure of data on laptops. In addition, the company is evaluating its privacy and data security program and making changes that will further enhance its protection of privacy and its handling of sensitive information.

## DICKSTEINSHAPIRO<sup>LLP</sup>

1625 Eye Street NW | Washington, DC 20006-5403  
tel: (202) 420-2200 | fax: (202) 420-2201 | dicksteinshapiro.com

March 19, 2008

Honorable Roy Cooper  
Attorney General of North Carolina  
Department of Justice  
9001 Main Service Center  
Raleigh, NC 27699-9001

Re: Recent Laptop Theft

Dear General Cooper:

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 21 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.

**DICKSTEINSHAPIRO LLP**

Honorable Roy Cooper

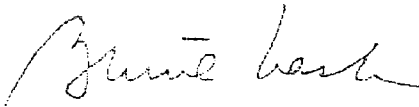
March 19, 2008

Page 2

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 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,



Bernard Nash

(202) 420-2209

nashb@dicksteinshapiro.com

Enclosure

Pfizer Inc  
235 East 42<sup>nd</sup> Street  
New York, NY 10017-5755

---

March 20, 2008

Sample Name  
Sample Address  
Sample City, State, Zip Code

Dear [\_\_\_\_\_]:

We are writing to let you know that a laptop stolen from a Pfizer contractor's locked home on February 7, 2008 unfortunately contained some of your personal information along with personal information belonging to approximately 800 present and former Pfizer employees and other individuals providing services to Pfizer. In particular, the laptop contained names and credit card numbers (mostly Corporate American Express card numbers), and in some cases, other personal information. Law enforcement was promptly informed and is still investigating. We are monitoring the matter and if there are significant developments, we will let you know.

We are not aware of incidents of fraud or identity theft resulting from this data loss. However, we want you to be alert to the possibility and we encourage you to take advantage of the support services that Pfizer is offering to help protect your identity and guard your credit.

Both Pfizer and our contractor deeply regret 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**

We are still analyzing a back-up copy of the data. Categories of information identified so far include:

*Name	*Credit card account number
*Credit card expiration date (month and year)	*Office and/or Home Address
*Office, Home and/or Cellular Telephone Number	*Office and/or Home e-mail addresses

We also have identified hotel loyalty program account numbers and other data, such as hotel preferences and other travel/logistics information. Please note that Social Security numbers, credit card PIN numbers or passwords do not appear to have been exposed. Since the laptop was not linked to a Pfizer computer system, we do not believe there is risk to other information about you that may be stored on Pfizer systems.

#### **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 has also 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. (Please see page 2 for registration instructions, including the registration deadline.) The IDS services include the following:

- **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 text alerts on your cellular phone 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. *NOTE: due to New York state law, this coverage is unavailable in New York.*

**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	<a href="http://www.equifax.com">www.equifax.com</a>
Experian	1-888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	1-800-680-7289	<a href="http://www.transunion.com">www.transunion.com</a>

- 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](http://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. Keep a copy of the report – you may need it for creditors. You also should file a complaint with the Federal Trade Commission at [www.ftc.gov/idtheft](http://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.

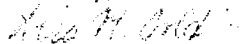
**Remember, the IDS credit protection services package is free to you. To register for credit protection support services, contact the Identity Safeguards Call Center at 866-910-5602, Monday – Friday, 9 am – 9 pm (ET). The registration deadline is September 30, 2008. To enroll, visit [www.idsaqi.com](http://www.idsaqi.com) and enter the access code provided below, disregarding any pricing information.**

Your Access Code: [insert access code]

Pfizer and its contractors are serious about data security and protecting the privacy of personal information. Pfizer has announced additional security requirements for contractors, and we are also implementing additional standards and procedures for handling sensitive personal and other information

Again, we regret any inconvenience and encourage you to take full advantage of the Pfizer-sponsored services and other resources to protect your personal information. If you have questions, please send an email to [privacy@pfizer.com](mailto:privacy@pfizer.com) or call our Helpline mailbox at 212 733-0228.

Sincerely,



Lisa M. Goldman  
Chief Privacy Officer