

**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:	<u>Pfizer Inc</u>	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
Address:	<u>235 East 42nd Street</u>	
	<u>New York, NY 10017-5755</u>	
Telephone:	<u>(212) 733-6640</u>	
Fax:	<u>(646) 792-4565</u>	
Email:	<u>Carlton.Wessel@Pfizer.com</u>	

Date Security Breach Reporting Form submitted: October 15, 2007

Date the Security Breach was discovered: August 18, 2007

Estimated number of affected individuals: 90

Estimated number of NC residents affected: 4

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 If so, please describe the security measures protecting the information: attached response

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: October 1, 2007

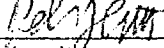
If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c): N/A

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:  Date: October 15, 2007

Contact Person, Title: Pete Levitas

Address: 1825 Eve Street, NW

(if different from above) 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
October 15, 2007

- Q. Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format:**
- A. It appears that the unauthorized data removal occurred when a departing Pfizer employee wrongfully arranged to have copies made of confidential information in electronic format from a Pfizer computer system on July 17, 2007, and did not return the information upon termination of employment on July 18, 2007. This was done in violation of Pfizer policy and in violation of the individual's employment contract. The sensitive personal information exposed related to approximately 90 current and former Pfizer colleagues, including 4 residents of North Carolina.
- 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 copied and removed from the Pfizer computer system was itself neither password protected nor encrypted. However, access to the information was restricted to those with appropriate authorizations, and those restrictions worked as anticipated; the security of the computer system was not breached. The copying of the information was completed on behalf of a person who was authorized to have such information at that time. The violation of Pfizer policy occurred after the information had been copied and delivered to that individual; specifically, the violation occurred when the individual retained the information after leaving the employ of Pfizer.
- 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 regulating employees' access to company computer systems and equipment, including access maintained by employees who are likely near the end of their Pfizer employment. 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.

Pfizer Inc.
Legal Division
215 East 42nd Street
New York, NY 10017-5755



Lisa M. Goldman
Chief Privacy Officer

September 28, 2007

Sample A. Sample
123 Any Street
Any Town, Any State Zip Code

Dear Sample:

We are writing to inform you of a recent incident involving the unauthorized removal of computer files from the Pfizer computer system by a departing Pfizer colleague. These files included your name and Social Security number ("SSN") as well as similar information for fewer than 100 other present or former Pfizer colleagues. We regret this incident and we apologize for any inconvenience that it may cause.

Details of Incident

On July 17, 2007 this individual (the "former colleague") made arrangements to have Pfizer business information and a small amount of personal information copied from the Pfizer computer system. At the time the copying occurred, the former colleague was under investigation for other matters, and may have concluded that termination of employment was a likely result. When the former colleague's employment ended on July 18, 2008, the former colleague kept that information, in violation of Pfizer policy and in violation of the former colleague's employment agreement. Pfizer discovered that information had been removed and, on August 3, 2007, demanded that it be returned but the former colleague claimed that the electronic copy of the information had been thrown out in the trash and was believed to have been destroyed. A forensic review of the computer system enabled us to determine, on August 18, 2007, that personal information was among the information copied from the system, including your name and SSN.

Pfizer is continuing to investigate this incident and we have already filed a lawsuit against the former colleague. One purpose of that lawsuit is to reduce the risk that the former colleague might share with anyone else the personal information that was removed from Pfizer. In addition, Pfizer has advised the three major U.S. credit bureaus about this incident. We gave a general report, alerting them to the fact that the incident occurred; Pfizer has not notified them about the presence of your specific information in the removed data. Pfizer has also notified the Attorney General's office in your state of residence about this incident, as well as other officials where required by law.

Despite our ongoing investigation, it is difficult to determine whether or not the copy of the information that was removed from Pfizer has actually been destroyed. However, to date we know of nothing to suggest that your personal information was accessed or acquired by any other unauthorized persons or that any unauthorized person, including the former colleague, has used or is misusing your information. Nonetheless, we are bringing this incident to your attention so that you can be alert to signs of possible misuse of your personal information.

Pfizer is also taking steps to help protect you from possible fraud and identity theft. Pfizer has retained Identity Safeguards ("IDS"), a specialist in identity theft protection, to provide you with two years of credit protection and credit restoration services, free of charge. You can enroll in the program by following the directions at the end of this letter.

Please keep this letter; you will need the personal access code it contains in order to register for services.

The IDS service package that Pfizer has arranged provides these protections for you:

- **Credit Monitoring:** IDS provides credit monitoring, which will give you unlimited access to your TransUnion credit report and score and will notify you via email of key changes in your TransUnion credit report that may indicate fraudulent activity.

Even if your credit report does not change, you will still 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:** Pfizer and IDS will arrange for the provision of \$50,000 of Identity Theft insurance with no deductible. This insurance provides reimbursement for costs incurred to restore your credit rating. *Please be aware, however, that due to New York state law, this coverage is not available in New York.*

Additional Ways to Help Protect Yourself

Besides registering for the free IDS credit protection services that Pfizer has arranged, there are other things that you can do to help protect yourself from fraud or identity theft.

We advise you to remain vigilant against the possibility of fraud and/or identity theft by monitoring your account statements and credit reports for unusual activity.

For your additional protection, you may want to contact the three major credit agencies to request that a "fraud alert" be placed on your credit file. A fraud alert is a consumer statement added to your credit file that warns creditors that you may be a victim of identity theft and requests that any creditors contact you before they open any new accounts or change your existing accounts. There is no charge for this service, and it is easy to request. Call any one of the three major credit agencies listed below. As soon as you alert one credit agency, it will notify the other two to place fraud alerts on your account as well. (Please note, however, that these procedures might cause some processing delay when you apply for credit. You should also activate the credit monitoring before placing fraud alerts to ensure faster and easier processing of the monitoring service)

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

You are entitled under U.S. law to one free credit report annually from each of the three major credit agencies listed above. Reviewing your credit report will allow you to confirm that no new accounts have been opened without your knowledge and may give you early notice of any potential fraud or incidents of identity theft. To order your free credit report, visit www.annualcreditreport.com or call toll-free 1-877-322-8228.

When you receive your credit reports, review them carefully. If you see anything you do not understand, call the credit reporting agency. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of Identity Theft. Make sure to obtain a copy of the

police report because you may need to provide the report to creditors to clear your record. 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). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

Even if you do not find suspicious activity on your initial credit reports, the FTC suggests that you keep checking your credit reports periodically. Identity thieves sometimes hold on to personal information for a period of time before using it. Checking your credit reports periodically can help you spot potential problems and address them quickly.

For additional information on how to further protect yourself against identity theft, you may wish to visit the web site of the FTC at www.ftc.gov/idtheft.

We encourage you to consider all options to help protect your privacy and security, and in particular, we encourage you to take advantage of the credit protection services we have arranged for you with IDS, at no charge to you.

How to Sign Up for the Free Credit Protection Services

You may sign up for the IDS credit protection services free of charge, either by calling IDS or visiting the website indicated below.

IDS has set up a Call Center with a special toll-free number (866-486-4810) to help you sign up and provide you with further assistance and information you may need regarding this incident and the free protections being made available to you. The IDS Call Center can be reached Monday-Friday, 9 am – 9 pm (ET).

You may also enroll on-line by visiting www.pflash.com. To sign up, just enter the access code provided below.

Your Access Code: [insert access code]

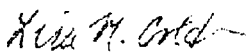
We encourage you to enroll and activate your credit monitoring quickly.

Please note that the deadline for enrolling in this service is March 31, 2008.

Pfizer understands how important it is to maintain the security and confidentiality of personal information. We are in the process of upgrading our computer security systems and privacy policies as part of our ongoing effort to improve data security throughout the Company. We will continue to assess this situation; should there be any significant developments regarding your personal information, we will notify you. If you have questions or wish to request more information from Pfizer, please send us an email at privacy.officer@pfizer.com or call us at (212) 733-0228.

Again, we regret any inconvenience that may result from this incident and encourage you to take full advantage of all resources to help protect your personal information.

Sincerely,



Lisa M. Goldman
Chief Privacy Officer