

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: June 15, 2007
Date the Security Breach was discovered: April 18, 2007
Estimated number of affected individuals: 17,000
Estimated number of NC residents affected: 569

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)): N/A

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: 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: June 5-8, 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))
 written notice
 electronic notice (email)
 telephone notice
 substitute notice
Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

Signature: Pete Levitas Date: June 15, 2007
Contact Person, Title: Pete Levitas
Address: 1825 Eye Street, NW
(if different from above) Washington, DC 20006-5403
Telephone: (202) 420-3495 Fax: (202) 420-2201 Email: levitasp@dicksteinshapiro.com

Addendum to North Carolina Security Breach Reporting Form

Filed by: Pfizer Inc

June 15, 2007

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

A. On March 26, 2007, the spouse of a Pfizer employee loaded unauthorized personal software onto a Pfizer laptop for the purpose of accessing a "peer to peer" file sharing network. That software gave other users of the file sharing network access to the contents of the employee's laptop, in electronic format, including information relating to approximately 17,000 individuals. Pfizer learned about the exposure of the data on April 18, 2007 and took action the same day to retrieve the laptop and prevent further exposure.

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 made accessible due to the unauthorized use of personal software was itself neither password-protected nor encrypted. However, the laptop at issue was equipped with a screensaver, which required the user's Windows domain password to unlock. This password was shared by the employee with the employee's spouse, who used it to access the machine.

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

A. Pfizer is implementing additional controls on its computer systems to restrict the ability to install unauthorized software, and ensuring that the source applications which generated the data on the laptop no longer use social security numbers. Moreover, a wide-ranging assessment is underway to determine if there are additional opportunities to enhance controls of sensitive company information. Pfizer is also updating its educational materials for all employees and contractors regarding the handling of sensitive information.

Pfizer Inc
235 East 42nd Street
New York, NY 10017-5755



June 1, 2007

Dear []:

We are writing to inform you of a recent incident involving the unauthorized disclosure of your name and Social Security Number ("SSN.") The information was stored on a Pfizer laptop computer that was provided to a Pfizer colleague for use in her home. Due to the unauthorized installation of certain file sharing software on the laptop, files stored in the laptop containing the names, SSNs, and in some instances, addresses and bonus information of approximately 17,000 present and former Pfizer colleagues were exposed to one or more third parties. Our investigation revealed that certain files containing your data were accessed and copied.

Details of Incident

Based on our investigation to date, we have no reason to believe that any other personally identifiable information was exposed. Also, because the laptop was being used to access the internet outside of the Pfizer network environment, there are no associated risks to any other data or systems maintained by Pfizer. We apologize for this incident and sincerely regret any inconvenience that these events and responding to this notice may cause you.

Keep in mind that Pfizer has no indication that any unauthorized individual has used or is using your personal information; we bring this incident to your attention, however, so that you can be alert to signs of possible misuse of your personal information.

Immediately after Pfizer learned of this incident we retrieved the laptop, disabled the unauthorized file sharing software, and conducted an investigation to determine which files, if any, were exposed. Although our investigation revealed that files containing names and SSN data were exposed to and, in some instances, accessed by one or more unauthorized persons over a "peer to peer" network, we are unable to determine the identity or location of those persons, or whether any particular file was opened or examined. Our investigation is on going, and we are taking steps to prevent any further dissemination of these files, and to determine the identity and location of any person(s) who may be re-posting them.

What Pfizer is Doing to Help Protect Your Privacy and Security

Under these circumstances, 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. To help you to protect yourself, Pfizer has taken the following steps:

- Pfizer has contracted with ConsumerInfo.com, Inc., an Experian[®] company, to provide you with one year of credit monitoring, at no cost to you. Provided you meet the standard eligibility requirements, you can elect at your option, to enroll in the program. ConsumerInfo.com, Inc. and Pfizer have set up a call center with a special toll-free number, **866-274-3891**, to provide you with

A1rev

further assistance and information you may need regarding this incident and the available protections.

- This credit monitoring product known as Triple Advantage™ Deluxe will identify and notify you of key changes in your three national credit reports that may indicate fraudulent activity. (Additional details appear below.) If you choose to enroll in the program, you will receive ongoing email or SMS/Text communications alerting you to any key changes to your credit reports from all three major credit agencies. Even if your credit reports do not change, you will still be updated on a monthly basis so that you can feel comfortable that your credit status has not been affected by this incident. Please contact ConsumerInfo.com, Inc. to enroll in this program at no cost to you.
- \$25,000 Identity Theft insurance provided by Virginia Surety Company, Inc. Please be aware, however, that due to New York state law restrictions, identity theft insurance coverage can not be offered to residents of New York.
- Pfizer has notified the Attorney General's office in your state of residence about this incident, and other officials where required by law. Those offices may offer further information and support to help you guard against fraud and identity theft.
- Pfizer has also contacted the three major U.S. credit agencies to inform them of this incident. This was a general report. None of your information was provided.

What You Can Do to Protect Yourself

For your additional protection, we suggest that you contact the fraud department at any one of the three credit agencies to inform them that you may be a potential victim of identify theft and 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 about possible fraudulent activity within your account 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.

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

In addition to the steps that Pfizer has already taken to protect you, there are a number of other ways you can protect yourself from fraud and identity theft:

- 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 (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 identify 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 any suspicious activity on your initial credit reports, the FTC recommends that you continue to check 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 U.S. Federal Trade Commission at www.ftc.gov/idtheft.

What Triple AdvantageSM Deluxe Includes

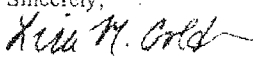
The credit monitoring product, Triple AdvantageSM Deluxe, will identify and notify you of key changes that may be a sign of identity theft. The package includes:

- o Unlimited access to your Experian Credit Report and Credit Score
- o Monitoring of ALL THREE of your national Credit Reports EVERY DAY
- o Email or SMS Text alerts when key changes are identified
- o \$25,000 Identity Theft insurance provided by Virginia Surety Company, Inc. (Due to state law restrictions, this coverage cannot be offered to NY residents.)
- o Access to Fraud Resolution Representatives

You have ninety (90) days to activate this service, which will continue for 12 months. We encourage you to activate your credit monitoring membership quickly. To register, please visit <http://partner.consumerinfo.com/pfizer> and enter the code provided below, disregarding any pricing information.

Your Credit Monitoring Access Code: [insert activation code]

Please rest assured that Pfizer takes data security very seriously and we have already taken steps to minimize any risk from this incident. In addition, we will continue to investigate and monitor this particular situation. Should there be any further significant developments in this matter, we will notify you. Again, we deeply apologize for any inconvenience or concern this incident may cause you, and we encourage you to take full advantage of the resources we have provided to protect your personal information.

Sincerely,


Pfizer Privacy Office
 By: Lisa M. Goldman

Pfizer Inc
235 East 42nd Street
New York, NY 10017-5755



June 1, 2007

Dear []:

We are writing to inform you of a recent incident involving the unauthorized disclosure of your name and Social Security Number ("SSN.") The information was stored on a Pfizer laptop computer that was provided to a Pfizer colleague for use in her home. Due to the unauthorized installation of certain file sharing software on the laptop, files stored in the laptop containing the names, SSNs, and in some instances, addresses and bonus information of approximately 17,000 present and former Pfizer colleagues were exposed to one or more third parties. Our investigation revealed that the files containing your data were exposed, but we are unable to determine whether they were accessed or copied.

Details of Incident

Based on our investigation to date, we have no reason to believe that any other personally identifiable information was exposed. Also, because the laptop was being used to access the internet outside of the Pfizer network environment, there are no associated risks to any other data or systems maintained by Pfizer. We apologize for this incident and sincerely regret any inconvenience that these events and responding to this notice may cause you.

Keep in mind that Pfizer has no indication that any unauthorized individual has used or is using your personal information; we bring this incident to your attention, however, so that you can be alert to signs of possible misuse of your personal information.

Immediately after Pfizer learned of this incident we retrieved the laptop, disabled the unauthorized file sharing software, and conducted an investigation to determine which files, if any, were exposed. Although our investigation revealed that files containing names and SSN data were exposed to and, in some instances, accessed by one or more unauthorized persons over a "peer to peer" network, we are unable to determine the identity or location of those persons, or whether any particular file was opened or examined. Our investigation is on going, and we are taking steps to prevent any further dissemination of these files, and to determine the identity and location of any person(s) who may be re-posting them.

What Pfizer is Doing to Help Protect Your Privacy and Security

Under these circumstances, 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. To help you to protect yourself, Pfizer has taken the following steps:

- Pfizer has contracted with ConsumerInfo.com, Inc., an Experian[®] company, to provide you with one year of credit monitoring, at no cost to you. Provided you meet the standard eligibility requirements, you can elect at your option, to enroll in the program. ConsumerInfo.com, Inc. and Pfizer have set up a call center with a special toll-free number, 866-274-3891, to provide you with

B2rev

further assistance and information you may need regarding this incident and the available protections.

- This credit monitoring product known as Triple AdvantageSM Deluxe will identify and notify you of key changes in your three national credit reports that may indicate fraudulent activity. (Additional details appear below.) If you choose to enroll in the program, you will receive ongoing email or SMS Text communications alerting you to any key changes to your credit reports from all three major credit agencies. Even if your credit reports do not change, you will still be updated on a monthly basis so that you can feel comfortable that your credit status has not been affected by this incident. Please contact ConsumerInfo.com, Inc. to enroll in this program at no cost to you.
- \$25,000 identity theft insurance with no deductible provided by a designated third party insurer. Please be aware, however, that due to New York state law restrictions, identity theft insurance coverage can not be offered to residents of New York.
- Pfizer has notified the Attorney General's office in your state of residence about this incident, and other officials where required by law. Those offices may offer further information and support to help you guard against fraud and identity theft.
- Pfizer has also contacted the three major U.S. credit agencies to inform them of this incident. This was a general report. None of your information was provided.

What You Can Do to Protect Yourself

For your additional protection, we suggest that you contact the fraud department at any one of the three credit agencies to inform them that you may be a potential victim of identify theft and 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 about possible fraudulent activity within your account 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.

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

In addition to the steps that Pfizer has already taken to protect you, there are a number of other ways you can protect yourself from fraud and identity theft:

- 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 [877-322-8228](tel:8773228228).
- 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 identify 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 any suspicious activity on your initial credit reports, the FTC recommends that you continue to check 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 U.S. Federal Trade Commission at www.ftc.gov/idtheft.

What Triple AdvantageSM Deluxe Includes

The credit monitoring product, Triple AdvantageSM Deluxe, will identify and notify you of key changes that may be a sign of identity theft. The package includes:

- Unlimited access to your Experian Credit Report and Credit Score
- Monitoring of ALL THREE of your national Credit Reports EVERY DAY
- Email or SMS Text alerts when key changes are identified
- \$25,000 Identity Theft insurance provided by Virginia Surety Company, Inc. (Due to state law restrictions, this coverage cannot be offered to NY residents.)
- Access to Fraud Resolution Representatives

You have ninety (90) days to activate this service, which will continue for 12 months. We encourage you to activate your credit monitoring membership quickly. To register, please visit <http://partner.consumerinfo.com/pfizer> and enter the code provided below, disregarding any pricing information.

Your Credit Monitoring Access Code: [insert activation code]

Please rest assured that Pfizer takes data security very seriously and we have already taken steps to minimize any risk from this incident. In addition, we will continue to investigate and monitor this particular situation. Should there be any further significant developments in this matter, we will notify you. Again, we deeply apologize for any inconvenience or concern this incident may cause you, and we encourage you to take full advantage of the resources we have provided to protect your personal information.

Sincerely,



Pfizer Privacy Office
By: Lisa M. Goldman