DICKSTEINSHAPIRO LLP

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

May 30, 2007

Via First Class Mail and E-mail

Honorable Kelly Ayotte
Attorney General of New Hampshire
State House Annex
33 Capitol Street
Concord, NH 03301-6397

Re: Pfizer Data Breach

Dear General Ayotte: Kelly

I am writing to give you advance notice of a data breach that has affected our client, Pfizer, as well as approximately 17,000 of its current and former employees ("employees"). It appears that approximately 98 of these employees are residents of your state. Pfizer plans to begin notifying the affected employees in the next several days. A copy of the notifications that will be sent are attached for your information.

The breach occurred when the spouse of a Pfizer employee loaded unauthorized software onto the employee's Pfizer laptop computer. This software allowed outsiders access to a number of files that included the names and social security numbers of the affected Pfizer employees. Based upon Pfizer's thorough investigation to this point, it appears that the affected employees can be grouped into two categories -- approximately 15,700 who actually had their data accessed and copied, and approximately 1,250 who may have had their data accessed and copied. Pfizer is notifying all of these employees with a letter describing the details of the data breach and also specifying whether the employee's data was actually accessed and copied. I am attaching copies of both letters. It appears that the data of 92 affected residents of your state was actually accessed and copied. With regard to both groups it is important to note that Pfizer has no evidence and no reason to believe that any unauthorized person has used any of the affected employees' personal information or that any personal information other than their names and social security numbers was accessed.

As you will note in greater detail from the attached letters, Pfizer has taken numerous steps to protect the security of the affected employees, including contacting the major national credit agencies and providing a full package of credit-protection services and credit insurance, free of charge. These protections will be available to all affected employees, in both categories.

Pfizer has taken steps to reduce the risk of future breaches and is continuing to carefully monitor this situation. Should any significant new information arise, we will promptly inform you. Please do not hesitate to contact me if I can provide you with any additional information at any time.

Best regards,

Bernard Nash
(202) 420-2209
nashb@dicksteinshapiro.com

Attachments (2)

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 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 same 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 Experian, one of the three major credit reporting agencies, to provide you support and protections at no cost to you. Provided you meet Experian's standard eligibility requirements, you can elect at your option, to enroll in Experian's program. Experian and Pfizer

have set up a call center with a special toll-free number, **866-274-3891,** to provide you with further assistance and information you may need regarding this incident and the available protections.

- Experian's support and protection package includes a credit monitoring program for one year. (Additional details appear below.) If you choose to enroll in the program, you will receive ongoing communications from Experian 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 Experian to enroll in this program at no cost to you.

- The support and protection package also includes a $25,000 insurance policy covering certain costs and expenses that you may incur as a result of this incident. Experian will provide details concerning eligibility requirements.

- 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 Experian's Services Include

Experian's credit monitoring product, Triple Advantage[SM], 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,

Lisa M. Goldman

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 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 same 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 Experian, one of the three major credit reporting agencies, to provide you support and protections at no cost to you. Provided you meet Experian's standard eligibility requirements, you can elect at your option, to enroll in Experian's program. Experian and Pfizer

have set up a call center with a special toll-free number, **866-274-3891**, to provide you with further assistance and information you may need regarding this incident and the available protections.

- Experian's support and protection package includes a credit monitoring program for one year. (Additional details appear below.) If you choose to enroll in the program, you will receive ongoing communications from Experian 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 Experian to enroll in this program at no cost to you.

- The support and protection package also includes a $25,000 insurance policy covering certain costs and expenses that you may incur as a result of this incident. Experian will provide details concerning eligibility requirements.

- 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 Experian's Services Include

Experian's credit monitoring product, Triple Advantage[SM], 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,

Lisa M. Goldman

Pfizer Privacy Office
By: Lisa M. Goldman