June 6, 2007

Bernard Nash, Esq.
Dickstein Shapiro LLP
1825 Eye Street NW
Washington, DC 20006

Re: Pfizer Security Breach

Dear Mr. Nash:

Thank you for your letter of May 30, 2007 regarding the recent data breach involving a number of current and former employees of your client, Pfizer, including 305 Connecticut residents. I appreciate Pfizer's efforts, set forth in the two employee letters attached to your correspondence, to notify all of the victims of this unfortunate data breach and to provide remedial measures such as credit monitoring and insurance at no cost to the victims.

I remain concerned about the possibility that credit card fraud and identity theft will arise from the breach of this personally identifying information. Accordingly, I ask that Pfizer also contact each of the Connecticut victims and inform them that under Connecticut General Statutes § 36a-701a, they may contact the credit bureaus listed below to request that a "Security Freeze" be placed on their credit report.

- Equifax Security Freeze
  P.O. Box 105788
  Atlanta, GA 30348
- Experian
  P.O. Box 9554
  Allen, TX 75013
- TransUnion Fraud Victim Assistance Department
  P.O. Box 6790
  Fullerton, CA 92834

I ask also that Pfizer consider reimbursing its employees for the cost of such a "Security Freeze," which prohibits credit bureaus from releasing a consumer's credit report or any information without the consumer's express authorization. The request must be made in writing to each credit bureau by certified mail and the credit bureaus

must place the security freeze on a consumer's credit report not later than five (5) business days after receipt of the request. Within ten days after placing a security freeze on a consumer account, the credit bureau must provide the consumer with written confirmation of the security freeze and a unique personal identification number (PIN), which the consumer will need any time he or she wishes to lift the freeze for a particular third party or period of time. Each credit bureau may charge a nominal fee to initiate or lift a freeze, for which Pfizer should be responsible for a reasonable period of time.

In addition, given the possible impact on consumers in Connecticut, my office is requesting that Pfizer provide more detailed information on how this breach occurred and what new procedures have been adopted to prevent future data theft. Please provide written answers to the following questions by June 22, 2007:

1. Prior to the breach of this data, what measures did Pfizer take to safeguard individuals' personally identifying information;
2. Please indicate how and when you first learned of this data breach;
3. Please describe how Pfizer was able to determine whether individuals' personally identifiable information was *actually* accessed and copied versus information that was *potentially* accessed and copied;
4. Please indicate if and when Pfizer first notified criminal authorities about this data breach;
5. Please describe in detail how the Pfizer laptop containing this personal data was compromised;
6. Please describe in detail the nature of the file sharing program that was on the laptop;
7. Please describe in detail the categories of information compromised by the data breach from the Pfizer laptop, such as, but not limited to, name, address, phone number, date of birth, driver's license number or other personal information;
8. Please identify whether other files were targeted, accessed, or copied in addition to those files that contained the personally identifiable information of current and former employees. If so, please describe the nature of that information;
9. Please describe all steps that Pfizer has taken to track down and retrieve the personally identifying information;
10. Please identify all steps Pfizer has taken or will take to contact and warn consumers that their personally identifying information may have been compromised, including but not limited to, when and how Pfizer first notified consumers of this data breach;
11. Please describe Experian's "standard eligibility requirements," and what provisions Pfizer is making to protect victims who may not satisfy these eligibility requirements;
12. Please identify what, if any, regulatory scheme Pfizer follows when responding to security breaches;

13. Please provide an outline of the plan your company has developed to prevent the reoccurrence of such a data breach and a timeline for implementing that plan; and
14. Please describe Pfizer's general corporate policies regarding securing computer systems, facilities, and personally identifying information.

As you are no doubt aware, the breach that occurred at Pfizer is only the latest in a disturbing series of cases where nonpublic personal information has been subjected to unauthorized access. In this era of increasing reliance on technology, as Pfizer unquestionably agrees, all companies entrusted with nonpublic personal information must employ the highest levels of security.

We anticipate and appreciate your client's cooperation in this matter and look forward to hearing from you. Please send the information requested in this letter to Assistant Attorney General Michael A. Martone at 110 Sherman Street, Hartford, Connecticut, 06105, (860) 808-5400.

Please do not hesitate to contact me or Attorney Martone if you have any questions.

Very truly yours,

RICHARD BLUMENTHAL

RB/pas