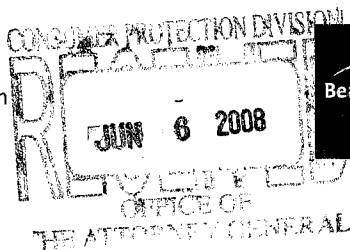


1676 International Drive
McLean, VA 22102

T 703 747 8000
F 703 747 8500
www.bearingpoint.com



Management
& Technology
Consultants

June 5, 2008

Hugh Williams
Identity Theft Program Coordinator
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Dear Mr. Williams:

I am writing on behalf of BearingPoint Inc. to inform you of a security breach affecting six Maryland residents. On May 14, 2008, the residence of one of our employees was burglarized and the company-issued laptop computer was taken amongst other personal property. The employee promptly reported the theft to the Atlanta Police Department, which is investigating the break in.

BearingPoint worked diligently to reconstruct the information stored on the stolen laptop. BearingPoint has been able to determine that the computer contains the name and social security number of independent contractors, including, as noted above, six Maryland residents. BearingPoint currently anticipates notifying affected individuals on or before June 6, 2008, of this incident. A copy of the letter that will be sent to the affected Maryland residents is attached.

If you have any questions concerning the matters discussed above, please do not hesitate to call me.

Very truly yours,

Sign By Order of Russ Berland, Chief Compliance Officer

A handwritten signature in black ink, appearing to read "Timothy Bowen". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Timothy Bowen
Director of Global Security and Investigations
(703) 747-3494

Dear _____:

Date:

BearingPoint recognizes the importance of safeguarding the personal information it handles in the course of conducting its business. To that end, we have implemented safeguards for that information. Even the most rigorous safeguards, however, can not guarantee protection against criminal conduct.

The Company was recently victimized by such conduct and we are writing to inform you that this criminal conduct might have a direct impact on you. On May 14, 2008, the residence of one of our employees was burglarized and the company-issued laptop computer was taken amongst other personal property. The employee promptly reported the theft to the Atlanta Police Department, which is investigating the break in. The investigation into the burglary is on-going and BearingPoint is cooperating fully.

BearingPoint has worked diligently to reconstruct the personal information stored on the stolen laptop. We recently determined that the laptop contained forms with the first and last name and Social Security Number of some independent BearingPoint contractors, including you. The stolen laptop did not contain credit or debit card numbers, or financial account numbers.

We have no reason to believe that the information stored on the stolen laptop was the target of the burglary or that the information has been misused. The personal information on the laptop can be accessed only with two passwords and two forms of authentication. In addition, the personal information was not stored in a single file or spreadsheet but dispersed among numerous files. To date, we have received no report indicating that the information stored on the laptops has been accessed or misused.

BearingPoint recognizes this development, and any related inconvenience, might be upsetting. We regret this incident has occurred and we apologize for any inconvenience it may cause you. As a result of this incident, we have taken immediate steps to review our current policies and procedures to further enhance security for personal data we handle and to reduce the risk of a recurrence.

To lessen the potential inconvenience to you and reduce the risk that you might be subjected to attempts to steal your identity, we have engaged ConsumerInfo.com, Inc., an Experian® company, to provide you with one year of credit monitoring, at no cost to you. This credit monitoring membership, known as Triple AdvantageSM Premium, will identify and notify you of key changes in your three national credit reports that may indicate fraudulent activity.

Your 12-month membership includes:

- Monitoring all three credit files with Experian, Equifax® and TransUnion® – everyday
- Your Experian, Equifax and TransUnion credit reports provided at sign up
- Email alerts of key changes indicating possible fraudulent activity
- Monthly "No Hit" alerts, if applicable
- Dedicated team of fraud resolution representatives for victims of identity theft

*Due to New York state law restrictions, identity theft insurance coverage cannot be offered to residents of New York.

You have ninety (90) days from the date of this letter to activate this membership, which will then continue for 12 full months. We encourage you to activate your credit monitoring membership quickly.

- A. To sign up online, please visit [URL] and follow the instructions. If you sign up online, all credit reports and alerts will be delivered via email.
- B. To sign up by telephone, dial XXX-XXX-XXXX. If you sign up by telephone, all credit reports and alerts will be delivered by the US Post Office.

Your Credit Monitoring Activation Code: [insert Activation code]

Checking your credit reports periodically can help you spot problems and address them quickly. You should also monitor your financial account statements and immediately report any suspicious or unusual activity to your financial institution.

You may also wish to place a fraud alert or credit freeze on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus listed below to place a fraud alert on your file. As soon as one credit bureau confirms your fraud alert, the others are notified. It should be noted that, although fraud alerts can help prevent fraudulent credit accounts from being opened in an individual's name, they also can delay that individual's own legitimate attempts to secure credit.

Equifax
800-525-6285

Experian
888-397-3742

TransUnionCorp
800-680-7289

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, contact law enforcement and file a police report. Get a copy of the police report; many creditors want the information it contains to absolve you of the fraudulent debts. You also can contact the Federal Trade Commission (FTC) to obtain additional information about how to protect yourself against the possibility of identity theft or to file an ID theft complaint through its Website at www.ftc.gov/idtheft; by telephone, at 1-877-ID-THEFT (877-438-4338); or by mail, at Federal Trade Commission, Consumer Response Center, Room 130-B, 600 Pennsylvania Avenue, N.W. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

You may also find the information in "Take Charge: Fighting Back Against Identity Theft," a comprehensive guide from the FTC available at its website, helpful to guard against and deal with identity theft.

Please contact BPT-FMGOICPrivacy@bearingpoint.com should you have additional questions regarding the circumstances of the incident.

Again, we apologize and regret any inconvenience this incident may cause you.

Sincerely,

Mark Mills
Senior Manager, Procurement

ADDITIONAL INFORMATION FOR MARYLAND RESIDENTS

You can contact the three national credit bureaus directly to place a fraud alert on your credit report as follows:

Equifax: P.O. Box 740241, Atlanta, GA 30374-0241; (800) 525-6285
Experian: P.O. Box 9532, Allen, TX 75013; (888) EXPERIAN (888-397-3742)
TransUnion: P.O. Box 6790, Fullerton, CA 92834; (800) 680-7289

You can contact Maryland's Office of Attorney General for more information about how to protect yourself against the possibility of identity theft as follows:

Consumer Protection Division
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
Toll-free: 1-888-743-0023
Consumer complaint hotline: (410) 528-8662
Identity Theft Unit: idtheft@oag.state.md.us