



EBARA TECHNOLOGIES INCORPORATED  
51 MAIN AVENUE  
SACRAMENTO, CA 95838 U.S.A.  
PHONE (916) 920-5451 FAX (916) 925-6654

June 18, 2008

Mr. Doug Gansler  
Attorney General  
Office of the Attorney General  
200 St. Paul Place  
Baltimore, MD 21202

**Re: Ebara Technologies, Inc. Potential Security Incident Regarding Protected Health Information**

Dear Mr. Gansler:

Ebara Technologies, Inc.'s Employee Medical Benefit Plan (the "Plan") is providing notice regarding a potential security breach at one of its vendors. The Plan's current and former participants' protected health information may have been subject to unauthorized access or acquisition as a result of a break-in and theft of computers at the offices of one of the Plan's vendors. The Plan will issue notice of this potential breach to each former and current participant on Friday, June 20, 2008. Our records indicate that two (2) Maryland residents were potentially affected. Enclosed, please find the letter that we will be sending via mail to potentially affected individuals and other governmental agencies. We will also contact each nationwide consumer reporting agency regarding this matter.

If you have any questions or need further information, please contact:

Anna Marie Vasquez  
Manager, Human Resources/Payroll  
Ebara Technologies, Inc.  
51 Main Avenue Sacramento, CA 95838  
avasquez@ebaratech.com  
916-923-7502

Sincerely,

Ebara Technologies, Inc.'s Employee Medical Benefit Plan

Enclosure



EBARA TECHNOLOGIES INCORPORATED  
51 MAIN AVENUE  
SACRAMENTO, CA 95838 U.S.A.  
PHONE (916) 920-5451 FAX (916) 925-6654

### **MARYLAND ADDENDUM**

In addition to the agencies mentioned in the adjoining letter you may also contact the Maryland Office of the Attorney General to obtain more information about steps you can take to avoid identity theft:

**Office of the Attorney General**  
200 St. Paul Place  
Baltimore, MC 21202  
(410) 576-6300 or 1 (888) 743-0023 toll-free in Maryland  
[www.oag.state.md.us](http://www.oag.state.md.us)



**EBARA Technologies Inc.**  
51 Main Avenue, Sacramento, CA 95838 USA  
PHONE: (916) 920-5451  
FAX: (916) 923-7560

June 19, 2008

Re: Ebara Technologies, Inc. Employee Medical Benefit Plan  
Potential Security Incident Regarding Protected Health Information

Dear Participant:

According to our records, you are a current or former participant in the Ebara Technologies, Inc. Employee Medical Benefit Plan (the "Plan"). The Plan is subject to a federal law known as the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HIPAA requires the Plan to take reasonable steps to ensure the privacy of your "protected health information." Protected health information means all individually identifiable health information transmitted or maintained by the Plan, regardless of form (oral, written, or electronic).

We are writing to let you know that your protected health information held by the Plan may have been subject to unauthorized access or acquisition as a result of a break-in and theft of computers at the offices of one of our external benefit administration vendors on Monday, May 26, 2008. The vendor previously provided administrative services to the Plan with respect to our flexible spending account program. The vendor also coordinated the Plan's insurance premium payments and enrollment of participants and dependents. If your dependents have been covered by the Plan, then the dependents' protected health information also may have been exposed by this incident. If any protected health information was taken from the vendor's offices, it may have included the name, address, Social Security number, and/or flexible spending claims reimbursement information of Plan participants and dependents.

Upon discovery the next morning, the vendor reported the break-in and theft immediately to the Walnut Creek Police Department, report number 08-12367, a copy of which you may obtain from the Walnut Creek Police Department (1666 N. Main St., Walnut Creek, CA 94596, 1-925-943-5844). Just days following the incident, the vendor installed a new security system. The Plan is continuing to monitor the vendor's response to this potential data breach to ensure proper steps are taken to protect against further unauthorized access, in addition to providing notice to potentially affected individuals.

At this time, we do not know whether the protected health information of any Plan participants or dependents was actually taken. However, out of an abundance of caution, we want to make you aware of the incident and the steps that you may want to take in order to guard against identity fraud.

To protect yourself against identity theft or other unauthorized use of personal information, you can take some simple steps. First, you can remain vigilant over the next 12 months and review your credit card bills and credit report for unauthorized activity. You should promptly report any suspected identity theft or fraud to your local police department, the U.S. Federal Trade Commission ([www.ftc.gov/credit](http://www.ftc.gov/credit)), and your bank or other financial institution. The U.S. Federal Trade Commission, Consumer Response Center, may be contacted at: 600 Pennsylvania Avenue, NW, Washington, DC 20580 ([www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)), 1-877-IDTHEFT (438-4338). You can also contact the Fraud Alert

phone line of one of the three national consumer reporting agencies (credit bureaus) by calling: Experian at 1-888-397-3742; Equifax at 1-800-525-6285; or TransUnion at 1-800-680-7289. You can obtain a 90-day Fraud Alert for your credit record by calling one of these agencies.

Second, you may wish to obtain a copy of your consumer credit report without charge. Under federal law, you are entitled to one free copy of your consumer credit report from each of the three national consumer reporting agencies each year. You may request your free annual consumer credit report by calling 1-877-FACT-ACT (1-877-322-8228) or by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com). You may want to obtain copies of your consumer credit report to ensure the accuracy of the report information.

If you actually become the victim of identity theft, you would have the right to obtain a police report. You may also wish to contact your credit card issuers and financial institutions to inform them of the incident.

If you actually become the victim of identity theft, you may also contact the fraud departments of the three national consumer reporting agencies. You would have the right to place a security freeze on your consumer report at no charge if you provide a copy of the police report. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent; however, please be aware that using a security freeze may delay your own ability to obtain credit. You may request a security freeze by sending your request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail to one of the addresses below. The following information should be included when requesting a security freeze (please note that, if you request a credit report or security freeze for your spouse or other dependent, this information should be provided for your spouse or dependent as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth (month, day and year); (4) current address for the past two years; and (5) any police report or complaint. The request should also include a copy of a government-issued identification card (such as a driver's license or military ID card), and a copy of a recent utility bill or a recent bank or insurance statement. Each copy should be legible, and it should display your name and current mailing address and the date the document was issued. The consumer reporting agency may charge a fee to place a security freeze or remove a freeze, unless you are a victim of identity theft or the spouse or other dependent of a victim of identity theft, and you have submitted a copy of a police report relating to the identity theft to the consumer reporting agency.

**Experian Security Freeze**  
P.O. Box 9554  
Allen, Texas 75013

[www.experian.com](http://www.experian.com)  
1-888-397-3742

**Equifax Security Freeze**  
P.O. Box 105788  
Atlanta, Georgia 30348

[www.equifax.com](http://www.equifax.com)  
1-800-525-6285

**TransUnion**  
Fraud Victim Assistance Dept.  
P.O. Box 6790  
Fullerton, California 92834-6790  
[www.transunion.com](http://www.transunion.com)  
1-800-680-7289

To learn more and to report incidents of identity theft, you can go to [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) or [www.ftc.gov/credit](http://www.ftc.gov/credit), or you can call 1-877-ID THEFT (1-877-438-4338).

If you have additional questions, please contact a representative of the Plan Administrator, Ebara Technologies, Inc., which is giving this notice on behalf of the Plan:

Anna Vasquez  
Manager, Human Resources/Payroll  
Ebara Technologies, Inc.  
51 Main Avenue, Sacramento, CA 95838  
916-923-7502 (phone)  
916-923-7560 (fax)

This letter may include an attached addendum if we believe your state requires additional notice. If this letter is not accompanied by an attached addendum, however, we do not presently believe your state requires additional notice.

We apologize for any inconvenience this possible security incident may cause you. Again, we want to emphasize that we do not know whether any Plan participants or dependents actually had their protected health information taken. We are providing this information to you out of an abundance of caution. We will provide you with further information when the Plan's former vendor provides it to us.

Sincerely,

**EBARA TECHNOLOGIES, INC. EMPLOYEE MEDICAL BENEFIT PLAN**