



**Peri D. Bridger**  
Senior Vice President & Chief Human Resources Officer

May 9, 2008

Dear Sodexo Employee,

This letter is to inform you of the recent theft of a Sodexo-owned laptop computer that may have contained a file with personal employee information relating to you. While we have not been able to confirm whether in fact this file was on the laptop, by this letter, we are advising you of the situation in order to provide you with an opportunity to take steps to protect yourself against the possible misuse of the information in this file.

We suggest that you immediately consider taking the steps outlined on the reverse side of this letter, "IMPORTANT STEPS TO HELP PREVENT FRAUD." That information includes an explanation as to measures you can take to protect yourself from identity theft. In addition, you have the right to obtain a copy of the police report filed in connection with the incident.

We are sorry that this has happened. We take very seriously the information security of all of our employees, clients and customers. We continuously enhance and update our information protection and security protocols. We are committed to ensuring that we have the procedures and processes in place to prevent this from happening again.

We have established a toll free hot line, 1-877-749-3330, for you to contact with questions related to this incidence.

Sincerely,

A handwritten signature in cursive script that reads "Peri Bridger".

Peri Bridger  
SVP and Chief Human Resources Officer



## IMPORTANT STEPS TO HELP PREVENT FRAUD

1. **Carefully review all of your banking and credit card account statements issued over the last three months and report any unauthorized transactions to your bank or credit card companies.** Although the information involved did not include banking account or credit card information, you should review your accounts to make certain there was not unauthorized or suspicious activity on those accounts.
2. **Notify your financial institution(s) and credit card companies that you received this notice.** This will provide them with notice that information relating to you may have been viewed or accessed by an unauthorized party.
3. **Contact the fraud department at the three major credit bureaus listed below and ask them to place a "fraud alert" or a "security freeze" on your credit file.** When you place an initial fraud alert with one of the bureaus, your request will automatically forward to the other bureaus which will also place fraud alerts on your credit file. You will need to contact each bureau to establish a security freeze. *Please note,* placing a fraud alert or security freeze will make it more difficult for a criminal to open a fraudulent account in your name, but it may also make it more difficult for you to open a new account as well, because extra steps will be required to verify your identity in connection with the credit approval process. You may wish to discuss with the credit bureau when you call how you might minimize inconveniences to you during the time the fraud alert or security freeze is active.

### For a Fraud Alert:

**Experian:** (888) 397-3742 or [www.experian.com](http://www.experian.com)  
**Equifax:** (877) 478-7625 or [www.equifax.com](http://www.equifax.com)  
**TransUnion:** (800) 680-7289 or [www.transunion.com](http://www.transunion.com)

### For a Security Freeze:

<b>Equifax Security Freeze</b>	<b>Experian Security Freeze</b>	<b>Trans Union Security Freeze</b>
P.O. Box 105788	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, CA 92834-6790

To request a security freeze, you must provide the following:

- full name, with middle initial and generation, such as JR, SR, II, III, etc.;
  - Social Security number and date of birth (month, day and year);
  - current address and previous addresses for the past two years;
  - \$5 fee or a valid investigative or incident report or complaint with a law enforcement agency or the DMV showing that you are a victim of actual identity theft; and
  - one copy of a government issued identification card, such as a driver's license, state or military ID card, etc., and one copy of a utility bill, bank or insurance statement.
4. **Obtain a copy of your credit report from each of the three major credit reporting agencies and review them to be sure they are accurate and include only authorized accounts.** You are entitled to one free copy of your report annually from each of the three credit bureaus listed above. To order reports, you may visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free (877) 322-8228. Carefully review your credit report to verify that your name, address, account, and any other information is accurate and notify the credit reporting agencies of any errors you detect.
  5. **Visit the Federal Trade Commission's ("FTC") website at [www.ftc.gov](http://www.ftc.gov) to obtain additional information about how to protect against identity theft.** You may also wish to contact the FTC at (877) FTC-HELP (877-382-4357) or TTY: (866) 653-4261 if you have further questions about identity theft.
  6. **Remain vigilant over the next 12 to 24 months and report any suspected incidents of identity theft or other misuse of personal information immediately.**