



RECEIVED
OFFICE OF THE ATTORNEY GENERAL
2008 MAY 12 P 1:47

Robert A. Stern
Senior Vice President and
General Counsel

May 9, 2008

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

Dear Attorney General Gansler:

We are writing to inform you, pursuant to the provisions of Maryland Statutes Section 14-3504(h), of an incident involving possible unauthorized access to personal information relating to 919 employees of Sodexo who reside in Maryland.

We are sending letters today to these employees to notify them of the theft of a Sodexo-owned laptop computer from the automobile of an employee of Sodexo in Montgomery County. This laptop may have contained an electronic file with the names and Social Security numbers of these employees. We have not uncovered any indication that the information was the target of the theft or that the information has been accessed or misused. The incident was reported to the Montgomery County Police Department and is under investigation.

We have not been able to confirm definitively that this file was on the laptop. But we have concluded that we should provide notice to the affected employees, both pursuant to Maryland law and to provide our employees with an opportunity to take steps to protect against possible misuse of the information. A copy of our notification letter is attached.

We are sending a separate letter today concerning this incident to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis (as defined in 15 U.S.C. § 1681a(p)).

Please let me know if you have any questions or if we can provide any additional information.

Sincerely,

A handwritten signature in black ink, appearing to read "Robert A. Stern".

Robert A. Stern



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. 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.

The laptop, along with other items, was stolen from the car of a Sodexo employee. We have determined that a file containing employee names and social security numbers may have been on the hard drive of the laptop. The file did not contain date of birth, home address, or other personal identification or personal financial information. The computer was password-protected. There is a risk, however, that a dedicated and computer savvy thief could circumvent this protection and gain access to files on the computer. The police are investigating the theft but to-date the stolen computer has not been recovered.

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.

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 the specific banking or credit card institution.** 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 one of the three major credit bureaus listed below and ask them to place a "fraud alert" 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. *Please note*, placing a fraud alert 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 is active.
 - **Experian:** (888) 397-3742 or www.experian.com
 - **Equifax:** (877) 478-7625 or www.equifax.com
 - **TransUnion:** (800) 680-7289 or www.transunion.com
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 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 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 general questions about identity theft.
6. Maryland residents may also wish to contact the Maryland Attorney General for more information about identity fraud and identity theft at: <http://www.oag.state.md.us/>

Main telephone number
(410) 576-6300 or 1 (888) 743-0023 toll-free in Maryland
TDD: (410) 576-6372

Mailing address:
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Remain vigilant over the next 12 to 24 months and report any suspected incidents of identity theft or other misuse of personal information immediately