June 3, 2009

Dear current employee:

We would like to inform you that a laptop computer containing information for current and former AARP staff was stolen from an AARP employee's residence on May 22, 2009. The computer contained data including your name, Social Security number, and date of birth. AARP's Information System, however, has not been compromised in any way. The local police department and the three consumer reporting agencies listed below have been notified of the theft.

We, at AARP, take the responsibility of safeguarding your data very seriously. As an immediate first step, AARP is procuring identity monitoring services through ID Analytics, an Identity Protection vendor, for everyone whose information was contained on the computer. Credit monitoring and, as needed, recovery and restoration services will also be provided. You will be enrolled in these services for one year at no cost to you. (After this one year period you will have no obligation to purchase anything, and you will not be approached by ID Analytics to do so.) Detailed information on ID Analytics and these services will be sent to all affected individuals. Individuals who wish to opt-out of these services may do so by contacting 1-800-514-4564.

While it is likely that the motive for the theft was the value of the computer itself, you are advised to monitor your banking and credit transactions for potential unauthorized activity. Because we all want to protect our personal data, especially if that data may have been compromised, we wanted to advise you of steps you can take to protect your personal information.

1. A security freeze allows you to prevent anyone from gaining access to your credit file to obtain new credit without your express authorization. This is especially important when someone who has access to your personal information seeks to get new credit in your name. While you can continue to obtain credit, this is a preventative measure against a form of identity theft. To place a security freeze on your credit file, you must contact each of the consumer reporting agencies listed below, and there may be a fee. The credit freeze will be in place until you take action to lift it.

2. You can also contact any one of the three consumer reporting agencies below and ask that they put a fraud alert on your credit file. While the fraud alert will not prevent creditors from gaining access to your credit file, it may prevent them from granting new credit in your name to an identity thief. While there is no fee for a fraud alert, it only lasts for a limited period of time and you will need to decide whether to contact one of the consumer reporting agencies when it expires to have it put in place again.

Consumer Reporting Agency	Equifax	Experian	Trans Union
Address	P.O. Box 740241 Atlanta, GA 30374-0241	P.O. Box 2104 Allen, TX 75013	P.O. Box 6790 Fullerton, CA 92834-6790
Phone	1-800-525-6285	1-888-EXPERIAN (1-888-397-3742)	1-800-680-7289

3. Call your bank(s) and any brokerage firms and ask them to put a password on your account so that inquiries, changes, or withdrawals cannot be made without the password.

When you get your credit reports, examine them for any accounts that you did not authorize or any other entries that may indicate that your personal information has been misused. You should also carefully examine any credit card or bank account statements for unauthorized charges.

If you suspect that you have actually been a victim of identity theft (maybe you see charges you didn't make on your credit card bill, you get a credit card bill or a call from a creditor about an account you never opened, and/or you didn't get an expected monthly credit card bill), you should do these things immediately:

1. File a report with your local police or the police where the identity theft took place. Get a copy of the report in case the bank, credit card company, or others need proof of the crime at a later time.

2. Use the Federal Trade Commission's Identity Theft Affidavit at www.consumer.gov/idtheft. (If you do not have access to the Internet, call us at the number below, and we will send a copy of this form to you immediately.)

3. Contact each of the fraud departments of the consumer reporting companies to report that you suspect that your identity has actually been stolen. If you haven't done so already, you can request a "fraud alert" be placed on your file.

4. For any accounts that have been fraudulently accessed or opened, contact the security departments of the appropriate creditors or financial institutions. Close these accounts. If you haven't already, put passwords (not your mother's maiden name) on any new accounts you open.

The Human Resources staff at AARP work very hard to protect the information of the people we employ and continue to take many precautions to protect your personal data. We sincerely apologize for this inconvenience.

If you have any questions concerning the details of this letter, please call AARP toll-free at 1-800-514-4564.

Sincerely,

B. J. Shelton

B. J. Shelton
Vice President, Human Resources