MCDSS MONTEREY COUNTY
DEPARTMENT OF SOCIAL SERVICES

WORKING TOGETHER FOR OUR COMMUNITY

1000 South Main Street, Suite 216
Salinas, California 93901
ph 831 755-4448 *fx* 831 755-8477

Elliott Robinson, Director

September 20, 2013

«Insert Address»

Dear «Insert Name»,

We are writing to you because of a recent computer security incident affecting a Monterey County computer.

A Monterey County computer that was connected to the California State Network was compromised the evening of 3/17/2013 by unauthorized users from overseas attempting to break-in over the network. This computer contained information on individuals who received public assistance benefits through Monterey County Department of Social Services between 2002 and 2009. This information included:

First and Last Name
Medi-Cal Identification Number
Address
Date of Birth

As soon as the County was notified on 3/18/2013 that unauthorized users were trying to access the computer, it was removed from the network in order to secure it from further compromise. Additionally, State network administrators have taken action to prevent similar attempts of unauthorized access.

An investigation into the incident was conducted to determine if any sensitive information on the computer was exposed. That investigation concluded that the unauthorized users were able to break through the password protection on the computer between 3/17/2013 and 3/18/2013. While we have been unable to determine that the data on the computer was retrieved or transferred by the unauthorized users, there is a possibility that the above personal information was accessed.

We have advised the California Attorney General's Office and the State Office of Privacy Protection about this incident. Because of the type of personal information on the computer, we recommend you consider taking the precautionary measures listed below.

RECOMMENDED PRECAUTIONARY MEASURES:

1) Place a Fraud alert and check your credit reports. You may place a fraud alert on your credit files and order a copy of your credit reports, at no cost to you, by following the steps outlined in the Privacy Protection Recommendations document that you received with this letter.

2) Continue to monitor your credit reports. Periodically check your credit reports and financial accounts for identity theft. Should you find suspicious activity on your credit reports, follow the steps outlined in the enclosure.

3) Keep a copy of this notice for your records. It is important for you to know that the personal information potentially exposed is limited to that previously described. These are the numbers of the major credit bureaus:

Trans Union -1-800-680-7289
Experian -1-888-397-3742
Equifax - 1-800-525-6285

More information on recommended privacy protection steps are outlined in the enclosure. For more information on identity theft, you may also visit the Web site of the California Office of Privacy Protection at www.privacy.ca.gov.

We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk that something like this could occur with any other County server or computer. Should you need any further information about this incident, the Monterey County Department of Social Services has set up a toll-free phone number (855) 670-9850.

Sincerely,

Elliott Robinson
Director

Enclosure [Privacy Protection Recommendations]

State of California
OFFICE of the ATTORNEY GENERAL
KAMALA D. HARRIS

Privacy Protection Recommendations

What to Do If Your Personal Information Is Compromised

1 Contact the three credit bureaus.

You can report the potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus. You will also be sent instructions on how to get a copy of your report from each of the credit bureaus.

Trans Union 1-800-680-7289 Experian 1-888-397-3742 Equifax 1-800-525-6285

2 What it means to put a fraud alert on your credit file.

A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that there may be fraud on the account. This alerts the merchant to take steps to verify the identity of the applicant. A fraud alert lasts 90 days and can be renewed.

3 Review your credit reports. Look through each one carefully.

Look for accounts you don't recognize, especially accounts opened recently. Look in the inquiries section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store names. The credit bureau will be able to tell you when that is the case. You may find some inquiries identified as "promotional." These occur when a company has obtained your name and address from a credit bureau to send you an offer of credit. Promotional inquiries are not signs of fraud. (You are automatically removed from lists to receive unsolicited offers of this kind when you place a fraud alert.) Also, as a general precaution, look in the personal information section for any address listed for you where you've never lived.

4 If you find items you don't understand on your report, call the credit bureau at the number on the report.

Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved and report the crime to your local police or sheriff's office.