Information Security Incident Involving Personal Information of IHSS Providers
Frequently Asked Questions for www.CDSS.ca.gov

1. What happened?

On May 9, 2012, CDSS was informed that there was a possible unauthorized release of personal information of In-Home Supportive Services (IHSS) providers and recipients. The information was in a package that was damaged in transit between a Hewlett Packard processing center and the State Compensation Insurance Fund. Upon arrival, it was noted that the package was damaged and that some of the information was missing. The information included IHSS providers' names and Social Security numbers as well as recipient's employer identification numbers. Reports have been filed with the United States Postal Service (USPS), the California Highway Patrol, the Office of Information Security and the State Information Officer.

2. When did it happen?

The package was mailed on April 26 and arrived on May 1, 2012. On Wednesday, May 9, 2012, CDSS was notified of the possible unauthorized release of your personal information.

3. Why did CDSS have my personal information?

Personal information including names and Social Security numbers are required to process and issue paychecks for work performed for IHSS recipients.

4. What personal information was released?

The documents that were missing contained the following information:

If you are an IHSS provider

- Your name
- Your Social Security number
- Your IHSS provider number
- Your IHSS case number
- If you are an IHSS recipient your employer identification number

5. Should I close my bank account, direct deposit or credit card accounts?

No, because your bank and credit card account numbers were not among the personal information items compromised in the breach. (As a general privacy protection measure, you should always look over your credit card bills carefully to see if there are any purchases you didn't make. If so, contact the card company immediately.)

6. Will this incident affect the processing of my IHSS timesheet or delay my IHSS paycheck?

No, this incident will have no impact on the processing of IHSS timesheets or issuing of paychecks.

7. How will CDSS prevent this from happening in the future?

CDSS, Adult Programs Division (APD) is working with its contractors to implement additional security practices in transporting confidential information. APD is also in the process of establishing new systems and processes that will eliminate the need for transporting this type of information in the future.

8. Does this mean that I am a victim of identity theft?
No. The fact that someone may have had access to your personal information does not mean that you are a victim of identity theft or that your information will be used to commit fraud. At this time, CDSS has no reason to believe that the data has been accessed or misused in any way. CDSS wanted to let you know about the incident so that you can take appropriate steps to protect your identity and credit. The way to protect your identity and credit is to request a fraud alert for your credit files, order a copy of your credit reports and review the reports to make sure they are correct.

9. What should I do to protect my personal information?
A letter is being sent to you about this incident which will include additional information that tells you what steps to take to request a fraud alert for your credit files. We also recommend that you regularly review activity on your credit card accounts and report any errors, incorrect information or unauthorized activity to your credit card company.

10. How will CDSS let me know if the information is found?
CDSS will provide updates on our website at www.CDSS.ca.gov with any new information that develops.

11. How will I know if any of my personal information was used by someone else?
The best way to find out if your personal information has been used without your authorization is to order a copy of your credit report from the three credit bureaus: Equifax, Experian and Trans Union. If you notice there are accounts on your credit report that you did not open or applications for credit ("inquiries") that you did not make, these could be signs that someone, other than yourself, is using your personal information without your permission.

12. Do I have to pay for a copy of my credit report?
No. You can order a copy of your credit report from all three credit bureaus for free once a year. You can do this online at www.annualcreditreport.com or by phone at 1-877-322-8228.

13. What else can I do to protect my personal information and identify?
You can request that a fraud alert be placed on your credit files. This is a free service. Simply call one of the three credit bureaus at the numbers provided below and follow the "fraud victim" instructions. The credit bureau you call will notify the other credit bureaus to place an alert on their credit files they have for you. When you call the credit bureau fraud line, you will be asked for identifying information and will be given the opportunity to enter a phone number for creditors to call. You may want to make this your cell phone number to make sure they can contact you, if necessary

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

You may also visit www.privacy.ca.gov for additional information about protecting your privacy.

14. I called the credit bureau fraud line and they asked for my social security number. Is it okay to give it?
The credit bureaus ask for your Social Security number and other information in

order to identify that you are the correct person and to make sure they do not send your credit report to the wrong person. It is okay to give this information to the credit bureau; providing that you initiated the call to them at one of the toll-free numbers noted above.

15. Do I have to call all three credit bureaus?
No. If you call just one of the credit bureaus, they will notify the other two credit bureaus. Each credit bureau will place an alert on their file of your credit report and you will receive a confirming letter from each credit bureau.

16. Why can't I talk to someone at the credit bureaus?
You must first order your credit report from the credit bureau to determine if there has been possible unauthorized use regarding your account. When you receive your report, it will have a phone number you can call to speak with a live person in the bureau's fraud unit. If you see anything on any of your reports that looks unusual or that you do not understand, call the number on the report immediately.

17. What is a fraud alert?
A fraud alert is a message that credit card companies receive when someone applies for new credit in your name. The message tells creditors that there is possible fraud associated with the account. They must take steps to verify the identity of the applicant. For example, they may call you at the phone number your provided when placing the fraud alert.

18. Will a fraud alert stop me from using my credit cards?
No. A fraud alert will not stop you from using your existing credit cards or other accounts. It may slow down your ability to get *new* credit. Its purpose is to prevent an unauthorized person to open credit accounts in your name. Credit card companies receive a special message which alerts them to the possibility of unauthorized use. Creditors know that they should re-verify the identity of the person applying for credit.

19. How long does a fraud alert last?
An initial fraud alert lasts 90 days. If you want to continue the alert after 90 days, you must call the credit bureau and request that the alert continue. There is no charge. You may also remove an alert by calling the credit bureaus at the phone number given on your credit report.

20. What if I have a fraud alert on, but I want to apply for credit?
You should still be able to get credit. While a fraud alert may slow down the application process, you can prove your identity to a prospective creditor by providing identifying information.

21. How long does it take to receive my credit reports?
You can view your reports online if you order them at www.annualcreditreport.com. If you order by phone, you should receive the reports by mail in five to ten days.

22. Should I contact the Social Security Administration and change my Social Security number?
The Social Security Administration very rarely changes a person's Social Security number. And the mere possibility of fraudulent use of your Social Security number would probably not be viewed as a justification for a new one. In addition, there are drawbacks to doing so. The absence of any history under the new Social Security number would

make it difficult to get credit, continue college, rent an apartment, open a bank account, get health insurance, etc. In most cases, receiving a new Social Security number would not be a good idea.

23. What should I look for on my credit report?

Look for any accounts that you do not recognize, especially accounts opened recently. Look at the inquiries or requests section for names of creditors from whom you have not requested credit. Note that some kinds of inquiries, labeled something like "promotional inquiries," are for unsolicited offers of credit, mostly from companies with whom you do business. Do not be concerned about those inquiries as a sign of fraud. (You are automatically removed from lists to receive unsolicited pre-approved credit offers when you put a fraud alert on your account. You can also stop those offers by calling 888-5OPTOUT [888-567-8688].)

Look in the personal information section to see if there are addresses listed where you have never lived. Any of these things might be indications of unauthorized use of your personal information. Also be on the alert for other possible signs of identity theft, such as calls from creditors or debt collectors about bills that you don't recognize, or unusual charges on your credit card bills.

24. What happens if I find out that I have been a victim of identity theft?

You should immediately notify your local law enforcement agency, contact any creditors involved and notify the credit bureaus. For more information on what to do, see the Identity Theft Victim Checklist on the Identity Theft page of the California Office of Privacy Protection's website at www.privacy.ca.gov. You may also call the Office of Privacy Protection at 866-785-9663.

25. How often should I order new credit reports and how long should I go on ordering them?

It might be a good idea to order copies of your credit reports every three months for a while. How long you continue to order them is up to you. Unauthorized use of credit generally occurs, but not always, soon after the personal information has been compromised. We recommend checking your credit reports at least twice a year as a general privacy protection measure.

26. Is there a number I can call if I need more information about this incident?

If you do not find the information you need in the letter we have sent to you or in the information provided by these FAQs, you may call: (888) 362-8947.

27. Why did it take so long to notify me of this incident?

It was important for CDSS to first verify that the personal information was released without authorization and take appropriate steps to notify all individuals.