Information Security Incident Involving Missing Storage Device
Frequently Asked Questions for WWW.Childsup.ca.gov

1. What happened?

On March 12, 2012, the Department of Child Support Services (DCSS) was notified by California's Office of Technology Services (OTech) that computerized storage devices being shipped from IBM to Iron Mountain were lost while being shipped by Federal Express. The storage devices were being returned from an IBM facility in Colorado, where the storage devices had been sent for purposes of a disaster recovery exercise At this time we do not believe the lost items were delivered to Iron Mountain.

2. When did it happen?

We were notified on March 12th that the storage devices were missing. It was confirmed on March 20th that the devices contained personal information. Since then we have been working to identify the individuals who are possibly affected by this incident. In addition, we have been working, together with our service providers, to see if the missing devices can be found—which is still a possibility. However, our primary goal has been to notify everyone as quickly as possible, and for that reason letters were mailed to all impacted parties on March 29, 2012. If the missing devices are found, we will provide appropriate updated information.

3. Why did you have my personal information?

Personal information is needed to conduct the activities of establishing and enforcing a child support case.

4. What specific items of personal information were involved?

The documents and forms that were on the missing device contained one or more of the following pieces of personal information:

- Name & Address
- Social Security Number
- Drivers License or Identification Number
- Name of Health Insurance Provider
- Health Insurance Plan Membership Identification Number
- Employer Information

The actual information for each participant will vary depending on what forms and documents were processed for their individual case.

5. How will you prevent this from happening in the future?

The California Office of Technology Services (OTech) is working with their contractors to strengthen their information security practices. OTech is also in the process of establishing new systems and processes that will eliminate the need for shipping storage devices in the future.

6. Does this mean that I'm a victim of identity theft?

No. The fact that someone may have had access to your information doesn't mean that you are a victim of identity theft or that your information will be used to commit fraud. At this time, we have no reason to believe that the data has been accessed or misused in any way.

We wanted to let you know about the incident so that you can take appropriate steps to protect yourself. The way to protect yourself is to place a fraud alert on your credit files, order your credit reports and review them for possible problems.

7. What should I do to protect my personal information?

An enclosure was included with the letter that we mailed you which outlines the steps you can take to place a fraud alert on your credit files. You may also visit www.privacy.ca.gov for additional information about protecting your privacy. We also recommend that you regularly review activity on your credit card accounts and report any fraudulent activity to the card issuer.

8. What should I do to protect the personal information of my child?

An outline of steps to take when your child's personal information is compromised is available on the Office of Privacy Protection's website at www.privacy.ca.gov. Or you may call the Office of Privacy Protection at 866-785-9663 for assistance.

9. How will you update me if the storage devices are found?

We will provide updates on our website at www.childsup.ca.gov with any new information that develops.

10. How will I know if any of my personal information was used by someone else?

The best way to find out is to order your credit reports from the three credit bureaus: Equifax, Experian and Trans Union. If you notice accounts on your credit report that you did not open or applications for credit ("inquiries") that you did not make, these could be indications that someone else is using your personal information, without your permission.

Also, regularly review the explanation of benefits statements you receive from your and your child's health insurer. If you see any service you believe you did not receive, please contact the health insurer at the number on the statement.

11. Do I have to pay for the credit report?

No. You can order your credit reports 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.

12. What else can I do to protect myself?

You can place a fraud alert on your credit files. Placing the fraud alert is free. Simply call any one of the three credit bureaus at the numbers provided below and follow the "fraud victim" instructions. The one you call will notify the others to place the alert. 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.

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

13. 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 you and avoid sending 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 we've provided.

14. Do I have to call all three credit bureaus?

No. If you call just one of the bureaus, they will notify the other two. A fraud alert will be placed on your file with all three and you will receive a confirming letter from all three.

15. Why can't I talk to someone at the credit bureaus?

You must first order your credit reports to determine if there has been possible fraud on your account. When you receive your reports, each one 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 don't understand, call the number on the report.

16. What is a fraud alert?

A fraud alert is a message that credit issuers 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.

17. 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 help protect you against an identity thief trying to open credit accounts in your name. Credit issuers get a special message which alerts them to the possibility of fraud. Creditors know that they should re-verify the identity of the person applying for credit.

18. How long does a fraud alert last?

An initial fraud alert lasts 90 days. If you want to reinstate the alert after 90 days, you may do so for free. You may also remove an alert by calling the credit bureaus at the phone number given on your credit report.

19. 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.

20. 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 10 days.

21. Should I contact the Social Security Administration and change my Social Security number?

The Social Security Administration very rarely changes a person's SSN. And the mere possibility of fraudulent use of your SSN would probably not be viewed as a justification. There are drawbacks to doing so. The absence of any history under the new SSN would make it difficult to get credit, continue college, rent an apartment, open a bank account, get health insurance, etc. In most cases, getting a new SSN would not be a good idea.

22. Should I close my bank account?

No, not unless your bank account number was among the items of personal information compromised in the breach. (As a general privacy protection measure, you should limit the use of your SSN where it's not required. For example, if your bank account number or PIN is your SSN, you should ask the bank to give you a different number. Do NOT use last four digits of your SSN, your mother's maiden name or your birth date as a password for financial transactions.)

23. Should I close my credit card or other accounts?

No, not unless your account number was among the items of personal information 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.)

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

Look for any accounts that you don't recognize, especially accounts opened recently. Look at the inquiries or requests section for names of creditors from whom you haven't 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.

Don't 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.)

Look in the personal information section for addresses where you've never lived. Any of these things might be indications of fraud. 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.

25. 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 Web site at www.privacy.ca.gov.

26. 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. Identity thieves usually, but not always, act soon after stealing personal information. We recommend checking your credit reports at least twice a year as a general privacy protection measure.

27. Is there a number I can call if I need more information about my child support case?

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: (866) 904-7674

28. When I call the Credit Bureaus, they want to sell me additional credit protection. Is that a good idea? Who should pay for it?

We don't believe that on-going credit protection service is needed for this incident. The missing tapes will require commercial level hardware and software to access and even then, each document on the tape must be examined individually. The chances of your personal information getting into the hands of an individual intending to commit identify theft is extremely small and practically non-existent. For these reasons, we do not recommend that you purchase additional coverage and for these reasons, the State of CA cannot arrange for the added service to be paid for on your behalf.

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

It was important for us first to verify that the tapes were actually lost and could not be found. Then, it was important for us to verify which customers were affected. And, finally, we had to make arrangements to get our notifications printed and mailed.