



Security Breach Frequently Asked Questions (FAQs)

- 1. *Who do I contact at CDPH regarding a breach of my personal or medical information held by CDPH?*** You would contact the particular CDPH program, office or unit named in CDPH Security Breach Notice you received. The program's contact information is listed at the bottom of the CDPH Security Breach Notice. A copy of the applicable Security Breach Notice regarding a breach of your personal or medical information held by CDPH may be accessed by clicking on the "[Security Breach Notices](#)". The Security Breach Notices are organized by the particular CDPH program, office or unit which is involved in the breach and the date of the security breach. You may also contact the CDPH Privacy Office:

California Department of Public Health
Office of Legal Services, Privacy Office
P.O.Box 997377, MS 0506
Sacramento, CA 95899-7377
E-mail: Privacy@cdph.ca.gov
Phone: (916) 440-7671, Toll Free: (877) 421-9634
Facsimile (FAX): (916) 440-7708

- 2. *How was my personal or medical information breached?*** Please review the security breach notice you received that explains how your personal or medical information was breached. The Security Breach Notices may be accessed by clicking on the "[Security Breach Notices](#)". The Security Breach Notices are organized by the particular CDPH program, office or unit which is involved in the breach and the date of the security breach.
- 3. *Why did you have my personal or medical information?*** In general, CDPH collects, uses and discloses your personal or medical information for a variety of public health-related purposes—and then only when authorized by law and pursuant to all applicable state and federal information privacy and security laws. With regard to a particular program at CDPH and why it collects, uses or discloses personal or medical information about you, please contact the particular CDPH program, office or unit named in the Security Breach Notice you received. This program contact information is listed at the bottom of each CDPH Security Breach Notice. A copy of the applicable Security Breach Notice regarding a breach of your personal information held by CDPH may be accessed by clicking on the "[Security Breach Notices](#)". The Security Breach Notices are organized by the particular CDPH program, office or unit which is involved in the breach and the date of the security breach.



- 4. *What specific items of my personal information were involved?*** The Security Breach Notice you received list specifically your personal or medical information that was breached. A copy of the applicable Security Breach Notice regarding a breach of your personal information held by CDPH. The Security Breach Notices may be accessed by clicking on the "[Security Breach Notices](#)" link. The Security Breach Notices are organized by the particular CDPH program, office or unit which is involved in the breach and the date of the security breach.
- 5. *What are you doing about the breach? How will you prevent this from happening in the future?*** The program and Information Security Office will conduct an investigation as to how the breach occurred. The program will revise or institute additional steps and policies to prevent or mitigate a reoccurrence. A copy of the applicable Security Breach Notice regarding a breach of your personal information held by CDPH may be accessed by clicking on the "[Security Breach Notices](#)". The Security Breach Notices are organized by the particular CDPH program, office or unit which is involved in the breach and the date of the security breach.
- 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 you are a victim of identity theft or that they intended to use the information to commit fraud. We wanted to let you know about the incident so you can take appropriate steps to protect yourself from identity theft by placing a fraud alert on your credit files and periodically reviewing your credit reports.
- 7. *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.
- 8. *Do I have to pay for the credit report?*** As a possible fraud victim, you are entitled to a free copy of your credit report. Simply call any one of the three credit bureaus at the numbers provided and follow the "fraud victim" instructions. You will automatically place a fraud alert on your credit file with all three of the bureaus.



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

You will soon receive a letter from each bureau confirming the fraud alert and telling you how to order a free copy of your credit report. Follow the instructions in the letters to receive your free reports. (Note: This free credit report that you're entitled to as a potential fraud victim is in addition to the free annual report that everyone is now entitled to. See www.oag.ca.gov/privacy for more info on the free annual report.)

- 9. *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 that you call.
- 10. *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.
- 11. *Why can't I talk to someone at the credit bureaus?*** You must first order your credit reports. 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.
- 12. *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 and gives them a phone number to call (yours) before issuing new credit. 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.



- 13. 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 alerting them to the possibility of fraud. Creditors know that they should re-verify the identity of the person applying for credit.
- 14. How long does a fraud alert last?** An initial fraud alert lasts 90 days. You can remove an alert by calling the credit bureaus at the phone number given on your credit report. If you want to reinstate the alert, you can do so.
- 15. 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.
- 16. How long does it take to receive my credit report?** It could take about 20 days from the day you call the credit bureaus. It takes about 5 to 10 days from the time you call the credit bureaus to get your fraud alert confirmation letter with instructions on ordering your credit report. You should receive your reports in another 5 to 10 days from the time you order them.
- 17. Should I contact the Social Security Administration and change my Social Security number?** The Social Security Administration very rarely changes a person's SSN. 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.
- 18. 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.)



- 19. *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.)
- 20. *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.
- 21. *What happens if I find out that I have been a victim of identify 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 Information-Sheet page of the California Office of Attorney General's Web site at <http://oag.ca.gov/idtheft/information-sheets>.
- 22. *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.



23. I heard that I could “freeze” my credit files. How does that work? A security freeze is a stronger measure than a fraud alert. A freeze prevents others from seeing your credit history without your permission. It costs \$10 to place a freeze with each of the three credit bureaus, for a total cost of \$30. You can also temporarily lift the freeze for \$10, if you want to apply for new credit yourself. For more information on the freeze, see Identity Theft Victim Checklist on the Information-Sheet Page of the Office of Attorney General’s Web site: <http://oag.ca.gov/idtheft/information-sheets>.

24. The notice is addressed to my child, who is a minor. What should I do? Call each of the credit bureaus at the numbers in the notice letter. Follow the fraud cues on the automated system and enter the child’s information. If you get a message of “report not found” or something like that, that’s good. That means your child doesn’t have a credit history. A creditor doing a credit check would get the same message, pretty much eliminating the risk of new credit being established in the child’s name. You might go through this process every few months for six months to a year.

If the fraud alert process goes through, then you’ll get a confirming letter in the mail from each of the credit bureaus with instructions for ordering your child’s credit report. Check the report(s) and call the credit bureaus about any information that looks suspicious or inaccurate.

25. The notice is addressed to my spouse, who is deceased. What should I do? Call each of the credit bureaus at the numbers in the notice letter. Follow the fraud cues and enter the deceased person’s information. If you get a message that says “reported deceased” or “no report on file” or something like that, that’s good. That means the credit bureaus have been notified by the Social Security Administration that the holder of the SSN is deceased. (Counties notify SSA when a death certificate is filed. The whole process can take months.) A creditor doing a credit check would get the same message, pretty much eliminating the risk of new credit being established in the person’s name/number.

If the fraud alert process on the automated phone system goes through, that may mean that the credit bureaus haven’t been notified of the death. In that case the spouse (or the executor of the estate) should notify the credit bureaus in writing that the person is deceased and that the person’s information may be at risk of identity theft. The credit bureaus will flag the file as deceased.



The spouse (or executor) must include the following information in the letters to the credit bureaus:

- Deceased's full name, date of birth, most recent address, and SSN
- Copy of the death certificate
- The spouse may request and receive a copy of the deceased's credit report at the spouse's home address.
- An executor wishing to receive a copy of the deceased's credit report should enclose a copy of the executorships' papers.

Mail to the credit bureau addresses below.

Credit Bureau Fraud Departments

	<i>Experian</i>	<i>Trans Union</i>	<i>Equifax</i>
Phone	888-397-3742	800-680-7289	800-525-6285
TDD	800-972-0322	877-553-7803	1-800-255-0056 & ask for Auto Disclosure Line, 800-685-1111
Address	P.O. Box 9532 Allen, TX 75013	P.O. Box 6790 Fullerton, CA 92834	P.O. Box 740241 Atlanta, GA 30374-0241