

Security Breach¹ Frequently Asked Questions

- 1. What happened?**
- 2. When did it happen? (Why didn't you notify me sooner?)**
- 3. Why did you have my personal information?**
- 4. What specific items of my personal information were involved?**
- 5. What are you doing about the breach? How will you prevent this from happening 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. 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. 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?**

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.
- 9. What else can I do to protect myself?**

You can place a fraud alert on your credit files. 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

¹ FAQs for incidents involving Social Security numbers only.

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**

10. 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.

11. 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.

12. 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.

13. 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 you provided when placing the fraud alert.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.)

20. 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.)

21. 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.

22. 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 Identity Theft page of the California Department of Justice's web site at www.oag.ca.gov .

23. 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.

24. 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 is the strongest protection available against identity thieves opening new accounts in your name. It costs \$10 to place a freeze with each of the three credit bureaus, for a total cost of \$30. (Or \$5 each, totaling \$15 for those 65 years of age or older.) 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 the California Department of Justice's *How to Freeze Your Credit Files* on the on the Identity Theft page of the California Department of Justice's web site at www.oag.ca.gov

25. The notice is addressed to my child, who is a minor. What should I do?

See the California Department of Justice's information sheet *When Your Child's Identity Is Stolen* on the Identity Theft page at www.oag.ca.gov.

26. The notice is addressed to my spouse, who is deceased. What should I do?

See the California Department of Justice's information sheet *Identity Theft and the Deceased* on the Identity Theft page at www.oag.ca.gov.