

Equifax Breach Q&A

1.	How do I find out if my information has been compromised?	Visit Equifax’s website, www.equifaxsecurity2017.com . Click on the “Potential Impact” tab and enter your last name and the last six digits of your Social Security number. Your Social Security number is sensitive information, so make sure you’re on a secure computer and an encrypted network connection any time you enter it. The site will tell you if you’ve been affected by this breach.
2.	What are some steps I can take protect myself after a data breach?	<ol style="list-style-type: none"> 1. Check your credit reports from Equifax, Experian, and TransUnion — for free — by visiting annualcreditreport.com. Accounts or activity that you don’t recognize could indicate identity theft. Visit IdentityTheft.gov to find out what to do. 2. Consider placing a credit freeze on your files. A credit freeze makes it harder for someone to open a new account in your name. Keep in mind that a credit freeze won’t prevent a thief from making charges to your existing accounts. 3. Monitor your existing credit card and bank accounts closely for charges you don’t recognize. 4. If you decide against a credit freeze, consider placing a fraud alert on your files. A fraud alert warns creditors that you may be an identity theft victim and that they should verify that anyone seeking credit in your name really is you. 5. File your taxes early — as soon as you have the tax information you need, before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS. 6. If you become the victim of identity theft outside of the tax system or believe you may be at risk due to a lost/stolen purse or wallet, questionable credit card activity or credit report, etc., you are encouraged to contact the IRS at the Identity Protection Specialized Unit, toll-free at 1-800-908-4490 so that the IRS can take steps to further secure your account. Please refer to the links below for further information. https://www.irs.gov/individuals/how-do-you-report-suspected-tax-fraud-activity and https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin and https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft <p>If you’ve been a victim of a data breach, keep in touch with the company to learn what it is doing to protect you and follow the “Steps for victims of identity theft.” Data breach victims should submit a Form 14039, Identity Theft Affidavit, only if your Social Security number has been compromised and your efile return was rejected as a duplicate or IRS has informed you that you may be a victim of tax-related identity theft.</p>
3.	How can I learn more about protecting myself after a data breach?	Visit Identitytheft.gov/databreach to learn more about protecting yourself after a data breach.
4.	How did Equifax get my information? Was it provided by Citizens 1 st Bank?	All financial institutions report to the major credit reporting agencies when you apply for a loan, a credit card, or a deposit account.

Source: Federal Trade Commission