

Equifax Data Breach Puts Millions at Risk

Close to half the population of the United States could be affected by a recent cyber attack on Equifax, one of the three largest American consumer credit reporting agencies in the United States. The company also provides identity theft protection.

Equifax announced on Thursday, September 7, 2017, that approximately 143 million U.S. consumers had their private information accessed between mid-May and July 2017.

This information includes:

- Names
- Social security numbers
- Birth dates
- Addresses
- Driver's license numbers
- Credit card numbers

ARE YOU AT RISK

If you have used Equifax's credit services, your personal information could be at risk.

To determine if your personal information may have been impacted by this incident, please follow the steps below:

1. Enter <https://www.equifaxsecurity2017.com> into your browser. Once you are on the webpage, click on the "Potential Impact" box located at the bottom left of the page and then click on the **CHECK POTENTIAL IMPACT** box found on the next screen. You will be asked to provide your last name and the last six digits of your Social Security number.
2. Based on that information, you will receive a message indicating whether your personal information may have been impacted by this incident.

Equifax will offer free identity theft protection and credit file monitoring to all U.S. consumers affected by the data breach.

For more information, please visit Equifax's website: <https://www.equifaxsecurity2017.com/>.

If you have additional questions, contact their dedicated call center at (866) 447-7559 from 6:00 am to 12:00 am, which is set up to assist consumers.

Noted below are some suggestions for actions that you can take to help protect your accounts, such as:

- **Personal credit reports should be monitored for new applications that were filed on your behalf.**
- **Monitor all monthly statements for any unauthorized payments.**
- **Monitor your existing credit card and Credit Union/bank accounts closely for charges you don't recognize; such as address or phone number changes.**
- **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.**
- **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 are you.**
- **File your taxes early – as soon as you have the tax information you need and 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. The IRS will only contact you through the mail.**