



From Your Trusted Identity Management Provider:
**Tips to Help You Deal with the
Equifax Data Breach**

**Information on how to better protect your identity
after this data breach event.**

Exactly what happened?

Credit reporting agency, Equifax, confirmed on September 7, 2017, that they experienced a massive data breach event potentially impacting 143 million American consumers, making it one of the largest electronic data breaches in U.S. history. The company also identified unauthorized access to limited personal information for certain residents of the United Kingdom and Canada.

What kind of information was exposed?

Equifax said that the breach primarily involved names, Social Security numbers, birthdates, addresses and, in some cases, driver's license numbers. The suspected criminal hacker or hackers behind the attack also gained access to a limited number of credit-card numbers along with certain dispute records with personal identifying information (PII).

How do I find out if I am affected by the breach incident?

You can visit the Equifax Potential Impact website page at <https://www.equifaxsecurity2017.com/potential-impact/> to determine if your personal information may have been impacted by this incident. Simply click on the "Potential Impact" link.

Should I check out my credit with all three bureaus?

We strongly recommend it. Most credit card issuers and lenders report consumer activity to all three major U.S. credit bureaus, and your data is likely duplicated at Experian and TransUnion. There's no reassurance in the fact that only one bureau was hacked.

How do I check all three?

You're entitled to at least one free credit report from each credit bureau every 12 months via AnnualCreditReport.com. If you haven't accessed your credit reports within the past 12 months, do it now. If you've reviewed them recently, placing a fraud alert on your credit files allows renewed access. Use your reports from the bureaus, and any free score and report services you have, to watch for:

- New accounts that you didn't open
- Credit inquiries that don't match when you applied for credit
- Balances that don't match your statements



How do I contact the Resolution Center?

Easy. Day or night, assistance from their dedicated expert, bilingual fraud resolution specialists is only a phone call away. If you need identity theft assistance and privacy management assistance, simply call us and as soon as your eligibility is verified, you'll be connected to an experience fraud specialist, who will provide unlimited assistance until your problem is resolved.

What will the Resolution Center do?

The in-house CyberScout Resolution Center provides proactive support to help minimize the risk of identity theft and fraud and jumps into action if and when you become a victim. They don't just dispense advice, they work with you side-by-side until your case is resolved. That means they take charge of the situation and work with you to full resolution, no matter how long the process takes, 24 hours a day, 7 days a week. CyberScout will:

- Make the calls
- Write the letters
- Help replace personal documents that are lost, stolen, or destroyed
- Talk to creditors, bill collectors, the IRS, doctors, and hospitals and medical providers
- Resolve any and all identity theft issues
- Provide an individual solution for each victim
- Offer complimentary access to FraudScout identity monitoring and protection services to victims of identity theft
- Help restore affected credit connected to identity theft
- Create a case against identity thieves

What's a credit freeze? Should I automatically lock down my data with a credit freeze?

A freeze makes your credit reports inaccessible to most people, with some exceptions. You can access your own records, as can pre-existing creditors, debt collectors and a few others. It has no effect on your credit score. It protects you because new lenders and credit furnishers can't view your credit history...so they're unlikely to approve a new credit line in your name.

You may want to consider a credit freeze, but it's entirely up to you. It may take some time for the freeze to lift, so you have to plan ahead.

Also, you may still be susceptible to credit fraud. A credit freeze won't affect your current accounts. If a thief steals the information on an existing account, your credit may be used without your permission. Additionally, a freeze will not prevent fraudulent use of your Social Security number or medical insurance.

Is there a less drastic alternative to a credit freeze?

If a freeze isn't right for you, a less severe alternative is a 90-day fraud alert, which tells potential creditors to verify your identity before issuing credit in your name. You simply notify one credit bureau that you want a fraud alert, and you'll get one at all three bureaus. And it's free. In addition, you should get in the habit of monitoring your credit so you catch problems early.

How do I take advantage of a credit freeze or 90-day fraud alert?

Contact each individual credit bureau directly:

- Equifax: 1-800-349-9960
- Experian: 1 888 397 3742
- TransUnion: 1-888-909-8872



What other tips can you offer to minimize my risk?

- **Review your credit report.** Identify the information it contains and what, if any, information was compromised. Look for any unauthorized activity, such as a change in address or telephone number or misuse of your Social Security number.
- **Pay extra attention to your account, billing statements, medical and claims statements, IRS statements, and any other cases where thieves can use your PII.** Check for charges that aren't yours or use of your Social Security number.
- **Change all user access credentials.** If you use the same passwords for financial institutions or insurance claims information, change them. Watch financial and medical statements—on paper and online—for unauthorized transactions. Watch out for suspicious email, phone and snail-mail scams. Enable text and email alerts when possible. Turn on two-factor authentication when possible.

How do I educate myself on the Equifax breach incident?

Find out as much as you can about the breach and how to help minimize your risk:

- For up-to-date information, you should regularly visit the Equifax information site at <https://www.equifaxsecurity2017.com/>.
- Be sure to visit the Federal Trade Commission site at <https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do>.
- Also, check out our Knowledge Center to learn about the best ways to minimize your risk and help protect your personal information.
- The news media is extensively covering the incident and a source for information.

What if I have additional questions or concerns?

- Should you have any questions, please contact us your earliest convenience and we will connect you to a CyberScout fraud specialist.