**Protect Your Identity and Personal Financial Information**

*"Last week, somebody stole my identity. This week, they begged me to take it back!"*

*—Anonymous*

Chances are, you were affected by [Equifax security breach](https://www.equifaxsecurity2017.com/) which impacted 143 million Americans, plus some Canadians and Brits with US dealings. The breach reportedly happened on July 29, 2017, although the public was not informed until early September. If you're not sure what to do about it, or whether you've done enough, this article can help you make choices and take steps to protect your sensitive financial information from being used against you.

**First, check to see if you could have been impacted.** You can [check here](https://www.equifaxsecurity2017.com/potential-impact/), although it "may" give you an inconclusive ("you may have been affected") answer. Keep in mind: virtually anyone with credit would be in the Equifax data base, since they are one of the big three credit bureaus monitoring credit activity of Americans. So even if you've never personally set up an account with Equifax, if you have a credit score or any current or recent credit instrument: a credit card, mortgage, car loan, or installment loan, *your personal information was probably compromised.*

**Check your credit report.** This won't tell you if someone has your information, but it will give you a "baseline" on your credit. Plus, if there are inaccuracies on it (new or old), you can file disputes and get it cleaned up. You can get a full, detailed credit report from the three credit bureaus once per year at no cost (FICO score is extra) at [AnnualCreditReport.com](https://www.annualcreditreport.com/index.action).

**Then, decide how to protect yourself for the long haul.** After all, protecting your personal financial information—your credit, identity, banking information, etc.—matters all of the time, not just following a security breach. So it may be time to put long-term protection in place. Seven options include:

**1. Accept Equifax's offer of credit monitoring and ID theft protection.**

Equifax is offering all customers potentially affected by the breach TrustedID Premier free for one year. There's no credit card information taken, and you won't automatically be charged when the year ends to continue it. You can [sign up for it here.](https://www.equifaxsecurity2017.com/enroll/) It includes:

* an Equifax credit report
* monitoring from all three bureaus (Equifax, Experian and TransUnion)
* an Equifax credit report lock (see below about locks/freezes)
* Social security number monitoring
* and $1 Million in identity theft insurance.

As we were writing this, we found articles warning *not* to sign up for Equifax credit monitoring because the "fine print" agreement prevented you from participating in any sort of class action lawsuit or taking any legal action at all, should you suffer financial damages from their compromised security. *This is no longer the case.* The clause has been removed, and the updated terms apply as well to anyone who signed up before the language was removed.

Signing up for [TrustedID Premier](https://www.equifaxsecurity2017.com/enroll/) is an option unless you have a more comprehensive solution in place. Be sure to check your credit report for any inaccuracies, and be aware to continue or replace this service at the end of the year if you don't have something similar in place.

**2. Monitor your own credit report.**

If you were not part of the breach and not eligible for (or do not want) Equifax's offer, there are many other ways to monitor your credit.

Some budget options: [CreditKarma.com](https://www.creditkarma.com/) offers daily credit monitoring from TransUnion plus tools and articles to help you raise your score... all at no cost. or you can sign up directly to [TrueIdentity](https://www.transunion.com/product/trueidentity-free-identity-protection) from TransUnion. (It's marketed as "free identity protection," but it's really little more than credit monitoring.)

Do be aware that free options are more likely to allow the credit monitor's "partners" to market to you, although you may be able to opt out of emails you do not want.

For paid options, we recommend services that will do *more* than merely monitor your credit, since protecting yourself from identity theft involves more than just watching your credit. So if you are "established" with multiple bank accounts, credit cards, etc., and can pay for a higher level of monitoring, we suggest the next option...

**3. Get identity theft protection and restoration.**

 Credit monitoring is important, but it won't do you much good as far as protecting your financial information, or assisting you if someone does indeed use your information—or worse, your identity—for theft or impersonation.

According to a new identity fraud study from Javelin Strategy & Research, in 2016, over 15 million Americans had their identities stolen, with losses of $16 billion dollars. Unfortunately, in spite of attempts to fight the crime of identity theft, these were new highs in both the number of people impacted and the amount stolen.

The Government Accountability Office recommends that, in addition to credit monitoring, a comprehensive solution also includes identity monitoring and identity restoration. Identity monitoring tracks your personal data on illicit websites as well as public records. Identity restoration services assist you in recovering from identity theft, and can include case management, legal help, and reimbursement for costs and losses.

Three top identity theft protection programs recommended by ASecureLife.com are:

* [IdentifyForce](https://www.identityforce.com/)
* [LifeLock](https://www.lifelock.com/)
* [IDShield](https://www.idshield.com/comparison-chart)

They all monitor your credit and also bank accounts, passport, drivers license, and more. IdentityForce is top rated, and IDShield is perhaps the best value for a comprehensive solution at $9.95/month or $19.95 for a family. You can [read a comparison here](http://www.asecurelife.com/identity-theft-protection-reviews/).

State Farm offers ID theft insurance for only $25/year as an add-on to home or condo insurance. However, by itself, this type of insurance is insufficient as it offers no monitoring and therefore won't help nip identity theft in the bud.

**4. Consider freezing or locking your credit.**

A credit freeze or lock will prevent anyone—even you—from using your social security number to obtain a new credit account in your name. If you are a long-term renter or homeowner with no plans to obtain additional credit (or don't mind the hassle if you do), it could be worth considering. However, it's not a bulletproof solution.

The advantage to a freeze is that no one can take new credit in your name. It doesn't affect your credit score and you can still obtain your own free annual credit report. The disadvantage is that it won't stop thieves from charging an existing line of credit, so you'll still want your credit accounts monitored.

If you do place a freeze, you've got to remember to "thaw" your credit a few days ahead of when you might need it. You also have to place freezes with each bureau separately, and there can be a nominal cost ($5-$10) to place the freeze, as well as sometimes remove the freeze, from your credit. This cost varies from state to state—see this [handy chart](https://www.transunion.com/credit-freeze/credit-freeze-information-by-state)—and has been waived for Equifax customers at the moment.

Here’s where you can go to sign up for a freeze at each of the three major credit bureaus:

* [Equifax freeze online](https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp)
* [Experian freeze online](https://www.experian.com/freeze/center.html)
* [TransUnion freeze online](https://www.transunion.com/credit-freeze/place-credit-freeze)

Or call…

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

**5. Consider placing a fraud alert on your credit report.**

If you don't want a freeze or lock on your credit—perhaps you are going to be applying to purchase a home or car soon, or you just don't want the hassle—you can place a fraud alert on your credit report. It's easy and free, and you only need to place it with one bureau, which will inform others.

With a fraud alert, your credit report is flagged, and creditors and lenders are then required to take extra steps to verify your identity. According to Lifehacker.com there are three types of alerts available:

* [Initial Fraud Alert,](http://www.consumer.ftc.gov/articles/0275-place-fraud-alert) which protects your credit from unverified access for at least 90 days and can be renewed.
* [Extended Fraud Alert.](http://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes) For victims of identity theft, an extended fraud alert protects your credit for seven years.
* [Active Duty Military Alert,](http://www.consumer.ftc.gov/articles/0273-active-duty-alerts) which lasts one year to protect the credit of military personnel while deployed.

Here’s where to go if you want to place a fraud alert on your report (only one is necessary):

* [Equifax fraud alert](https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp)
* [Experian fraud alert](https://www.experian.com/fraud/center.html)
* [TransUnion fraud alert](https://www.transunion.com/fraud-victim-resource/place-fraud-alert)

(Or use the phone numbers above.)

You don't need a fraud alert if you've done a freeze... a freeze makes an alert unnecessary.

#### 6. ****Be vigilant about monitoring your own sensitive information.****

Monitoring companies can do a lot, but only you know what you’ve actually purchased or withdrawn. So keep your eyes open and don’t ignore anything that seems “not quite right.” Some suggestions:

* Check your bank accounts weekly or at least monthly.
* Monitor your investment accounts regularly for any unusual activity.
* Watch your mail for anything suspicious.
* Follow up on alerts from credit monitoring companies even if you think it's your own activity.
* [Get your annual Social Security benefits statement online](https://secure.ssa.gov/RIL/SiView.do) and look for anything unusual.
* NEVER give out your personal information to anyone who has not been sufficiently verified first. (And if you’re getting annoying calls from “the IRS”, it’s almost surely a tax scam.)

**7. Make protecting your information a lifelong habit.**

Unfortunately, this is not a temporary drill. As Alex McGeorge, the head of threat intelligence for Immunity security firm told Wired.com, “Your Social Security number doesn’t change, so this data is going to get resold on the black market and hold its value for a while." Realize that your information could be circulating for years, so take steps to protect it. Credit and identity monitoring and protection is the new normal.

Finding out your sensitive information has been hacked is no fun! However, taking action to protect yourself is a positive step that can increase your peace of mind, minimize future hacks, and position you for a quick recovery even in a worse-case scenario.

**Secure and Protect Your Wealth**

Nobody wants a hacker or thief to be able to take their personal information or worse, take money from an account or credit card! And yet, many investors put their money where it can easily be lost to the whims of the market or eroded by inflation.

If you have savings earning virtually nothing in a bank account, or investments subject to risk and unexpected losses, contact us today. We can help you protect your money!

© Prosperity Economics Movement