

# HOW TO PROTECT YOUR CREDIT

*By Jacob Ansel*

**THE EQUIFAX BREACH AFFECTED** 145 million Americans, almost half the U.S. population. Even if Equifax says you weren't compromised, don't be lulled into a false sense of security. Protecting yourself is imperative whether you were impacted or not. If you haven't already, the best way to protect yourself is to place a security freeze on your credit files at the big three credit reporting bureaus.

Let's backtrack a bit. What exactly happened at Equifax? The consumer credit reporting agency – who along with TransUnion and Experian determine who can get a credit card, buy a home, refinance a mortgage, start a business – was hacked. Our social security numbers, birth dates, addresses, driver's license info, and credit card numbers were stolen. The breach lasted from mid-May through July before Equifax 'fessed up.

What steps can you take to keep your identity safe? Let's start with the IRS which has a program to protect your identity from someone filing fraudulent returns. There are millions of cases every year of folks filing false returns and getting refunds before the real return is filed. The IRS can issue you a PIN and returns can only be filed with that number which changes annually. It's a simple form mailed only to the address on the tax return. Go to the IRS website and type in IPIN. Another smart and simple suggestion is to file your taxes before scammers do.

The IRS will never call you unless they're working on an active case or have an agent assigned to you so don't fall for phone scams by divulging sensitive information. Millions have. If you're not sure if it's a real call, hang up and call the IRS at (800) 829-1040 and ask if you have any pending issues with them.

*Jacob Ansel, CPA, is a partner at Vision Financial Group CPAs LLP, an accounting, tax, and consulting firm. A frequent seminar speaker, Ansel has created analytical systems for business.*
***www.vfgcpas.com***

***You're 11 times more likely to be a victim of identity fraud if your data was breached during the Equifax hack. Deciding between monitoring or freezing credit has become a part of the national conversation as we settle into yet another cost of living in a digital world.***

One of the best ways to protect yourself against general credit hacking or theft is to sign up with an identity theft protection service, like LifeLock. They place an immediate freeze on your credit which no one can access unless you give the go ahead. A tax return can't be filed, a credit card can't be opened, absolutely nothing can be done without your permission. It freezes your credit with all reporting agencies.

If you decide against a credit freeze, at least consider placing a fraud alert on your files. A fraud alert warns creditors that you may be an identity theft victim and they should verify that anyone seeking credit in your name is really you.

The SEC requires mutual funds companies to identify, detect, and respond to red flags of identity theft, but they aren't required to restore assets stolen by hackers. You should call your 401(k) plan provider and other investment managers to learn their fraud protection policies, which varies from company to company. If your investment company doesn't explicitly reimburse stolen funds, consider moving your money elsewhere.

Managing your smartphone and email accounts are critical to online security. Your phone is where all your second-factor text message codes are sent and where your mobile banking and other money apps live. Email is where your financial institutions send alerts and password reset links. Hackers can highjack your phone and access important information. Activate two-factor authentication on your email account. Download an authenticator app such as Google Authenticator or Microsoft Authenticator, which generates codes without the need for texts, which can be intercepted.

There are myriad steps to protect yourself and mitigate potential damage by the Equifax hack or any security breach. You should check your credit score every six months to make sure every inquiry and open balance belongs to you. Put a strong password on all computers and devices. Hackers can get into your laptop or home computer and steal your info from those sources. Don't think that because it's in your home you're safe. Don't leave anything with your social security number on your computer without a strong password. Use software with firewalls and a strong antivirus program. Never answer a credit card solicitation by mail or email.

It's surprising how many people I've spoken to who haven't taken action after the Equifax hack. Everyone's affected by identity theft and must take these breaches seriously. ❑