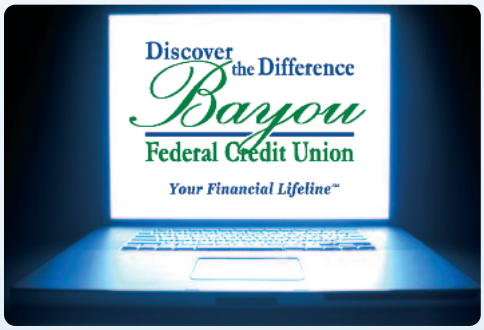
Equifax Breach UPDATE

October 13, 2017



Here is some more information on the Equifax Breach and how you may protect yourself in the aftermath...

What could happen?

The Equifax breach gave criminals access to vital personal information, including names, social security numbers, birthdates, addresses, and in some cases, driver's license IDs and credit card numbers. And here's just a slice of what those jerks can do with that data:

- Open financial accounts
- Apply for credit cards, mortgages, and other financial services
- Get medical care at your expense
- File for a tax refund in your name
- Get a job in your name and let you pay the taxes
- Steal your benefits
- All of the above (aka, identity theft)

How to protect yourself

One recommendation is to freeze your credit immediately with all four of the major credit bureaus. By freezing your credit, you'll prevent criminals from trying to open up new accounts in your name—all of your current credit cards will still work. You'll only need to consider unfreezing your credit if you want to apply for a loan, open a new credit card, or make any type of purchase that requires a check on your credit.

Three things you'll want to know before contacting the credit bureaus:

1. You'll want to pull a credit report. We recommend you pull one report now, another one in four months, and the third in another four months. It's not foolproof, but it will allow you to see different reports throughout the year to track any potential changes.

2. The cost is minimal. While reports have varied—Equifax is offering their credit freeze for free, but it's pretty hard to get through to them—freezing credit usually only costs a one-time fee of $10 per bureau. That's 20 or 30 bucks for a whole lot of peace of mind.

3. You must set or receive PINs when freezing your credit. Save these in a secure location, whether that's using a password manager or physically storing the printed PIN paper someplace safe and out of sight.

Where to go to freeze your credit

- Equifax: (800) 685-1111 or https://www.freeze.equifax.com/
- Experian: (888) 397-3742 or https://www.experian.com/ncaconline/freeze
- TransUnion: (888) 909-8872 or https://freeze.transunion.com/
- Innovis: (800) 540-2505 or https://www.innovis.com/securityFreeze

Additional monitoring services

The use of additional monitoring services is entirely up to you. Please make sure that you do your homework and research on these companies before signing up blindly out of fear.

When looking up information about how to protect yourself in situations like these, look to sites like the Federal Trade Commission or other technology publications such as Wired, The Verge, or Vice's Motherboard, as they won't be trying to upsell you to credit protection you may or may not need.

Additional tips and information:

Scams

Be on the alert for credit scams or any related terms. You'll see these in emails, ads on social sites or games, and even physical mail to your home. These attacks are part of what we refer to as social engineering, and they will run rampant for many months and years to come. Always be skeptical, and if you're not sure about something, ask a professional.

Phone or text scams

Since your data was most likely taken, that means your numbers will be shared even more than they already are today. Calls and texts from unknown numbers, numbers with similar area codes, or numbers very similar to yours should be treated as potential scams. You might think that the National Do Not Call Registry would protect you from this. Sadly, it does not. It offers protection from legitimate companies trying to solicit your business. It does not offer protection against scammers. (Because why would criminals follow the law, anyway?)

My Social Security account

The my Social Security account allows you to keep track of the social security funds you'll be collecting in the future. Although it was not affected by the Equifax breach, it's good practice to get this account set up in your name, as someone else could easily grab it and you'd be locked out of your future payments. One caveat: If you want to set up this account, you'll need to do it before you freeze your credit. (Otherwise they can't confirm your identity through the account.)

Passwords and two-factor authentication

Ensure you're using smart password strategy (complex, do not repeat them, do not use the same one across multiple sites/services, etc.) and if available, enable two-factor authentication (2FA) on every account possible.

Enable alerts on your accounts

While your current accounts shouldn't be impacted by this breach, it's never a bad idea to keep an eye on your bank accounts and credit cards for larger purchases. For accounts rarely used, you could set alerts to $1 so you're notified the second any transaction happens. For regular accounts, set the alerts to a dollar amount that would seem out of place for that card, whether it's $20 or $500.

New phone accounts

A common attack vector with credit/personal data breaches is to purchase new phone accounts through your provider, with your account! Once criminals have your info, they'll call up the phone company and say they want to add a new line but don't have a PIN number. If you haven't set up a PIN number with your phone company already, they have no way to verify your account. So guess what? BAM! There's a new phone on your bill. In order to protect yourself from this type of attack, go ahead and set up a PIN with your provider.

Taxes

File these as soon as possible next year! For multiple years we've heard about victims of tax return fraud, wherein a scammer using your personal information files YOUR return before you can. So don't wait on this one.

Summary

Remember, one new credit card created by an attacker in your name is going to cause a massive headache. Better to stay ahead of it than spend the next month trying to convince a bank or credit union that you didn't open an account. Take some time now to protect yourself and your accounts. It will be worth it.

For More Information

If you believe you are the victim of identity theft, you should contact the proper law enforcement authorities, including local law enforcement, and you should consider contacting your state attorney general and/or the Federal Trade Commission ("FTC"). You also may contact the FTC to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft