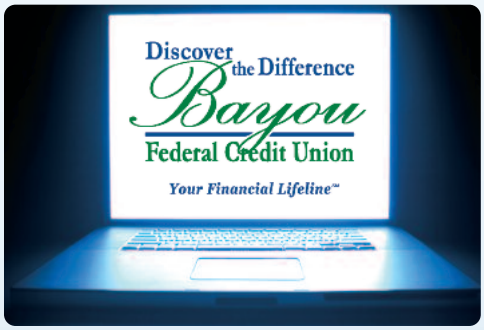
Equifax Breach
UPDATE 2

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.

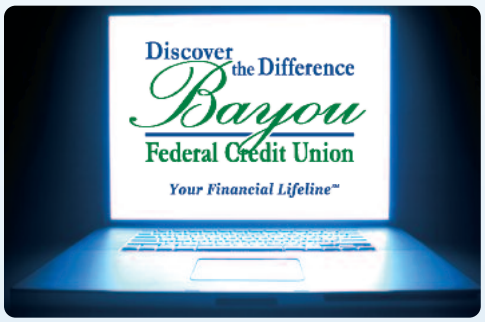
For More Information

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

Equifax Breach UPDATE

September 28, 2017



Earlier this year, Equifax, one of the 4 US credit bureaus, was the victim of a major data breach involving as many as 143 million records. This breach is more severe than most any other that has happened because of the amount and type of the data that Equifax collects. Data lost includes addresses, social security numbers, birth dates, credit card numbers, even driver's license numbers … everything you would ever need for identity theft and fraud.

At Bayou Federal Credit Union, protecting your accounts and your information is a top priority. That's why we want to share with you a few steps you can take to protect yourself against identity theft and fraud.

Check your credit reports

Each credit bureau is required to provide you with 1 free report every year. Visit **annualcreditreport.com** to get your free report. Again, this is free. If you are being told to pay for something, then you are on the wrong site.

Freeze your credit

If you don't plan on buying a house or car or want to get a new credit card then you could lock your credit report from being accessed without a special PIN. In Michigan this costs $10 per bureau to freeze, other states may vary.

To freeze your credit, call these credit bureaus:

Equifax (800) 685-1111 • Experian (888) 397-3742 • TransUnion (888) 909-8872 • Innovis (800) 540-2505

Fraud Alert

If you are in the process of buying a house or need your credit accessible to creditors you could alternatively place a Fraud Alert on your credit. These require creditors to alert you when your credit is being pulled. These only last for 90 days but can be renewed continually for free.

Be vigilant

There will undoubtedly be many email and phone scams using this event to coerce people into giving up money or information. Be skeptical of anyone asking for your personal or banking information.

File your taxes

File your taxes as early as possible. The stolen data would be enough for hackers to file false tax returns.

Credit Monitoring

Credit Monitoring can be comforting, but it only alerts you after someone has stolen your identity. If this happens to you, the crime has already been committed and Equifax is only offering free monitoring for 1 year. Your name, date of birth, social security number, and other personal information can still be vulnerable after that.

For More Information

If you have additional questions, call the Equifax dedicated call center at 866-447-7559, available from 7:00 a.m. to 1:00 a.m. Eastern time, seven days a week.

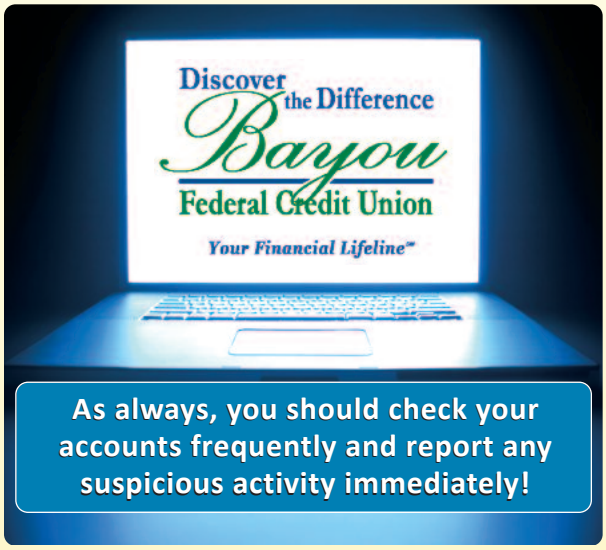
Bayou Federal Credit Union recommends that you always remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports.

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

Equifax Breach ALERT

September 8, 2017



Alert Summary

On July 29, 2017, Equifax discovered that criminals exploited a U.S. website application vulnerability to gain access to certain files. Upon discovery, Equifax acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm which has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017.

What Information Was Involved

Most of the consumer information accessed includes names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 consumers and certain dispute documents, which included personal identifying information, for approximately 182,000 consumers were accessed. In addition to this site, Equifax will send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted. No evidence of unauthorized access to Equifax's core consumer or commercial credit reporting databases has been found.

What Equifax is Doing

Equifax has established a dedicated website, **www.equifaxsecurity2017.com** to help consumers.

There is a tool on this site for you to determine if your information was potentially impacted by this incident.

To find out if you are potentially impacted, please go to www.equifaxsecurity2017.com, and click on "Potential Impact," and enter your last name and last 6 digits of your Social Security number.

Equifax is also offering free identity theft protection and credit file monitoring to all U.S. consumers, even if you are not impacted by this incident. This offering, called **TrustedID Premier,** includes 3-Bureau credit monitoring of your Equifax, Experian and TransUnion credit reports; copies of your Equifax credit report; the ability to lock and unlock your Equifax credit report; identity theft insurance; and Internet scanning for your Social Security number – all complimentary to U.S. consumers for one year. You must complete the enrollment process by November 21, 2017.

What You Can Do

Visit the Equifax website, www.equifaxsecurity2017.com, then click on "Potential Impact," and enter your last name and last 6 digits of your Social Security number.

In addition, please monitor your account statements and report any unauthorized charges to your credit card companies and financial institutions.

For More Information

If you have additional questions, call the Equifax dedicated call center at 866-447-7559, available from 7:00 a.m. to 1:00 a.m. Eastern time, seven days a week.

Identity Theft Prevention Tips

Bayou Federal Credit Union recommends that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports.

You may obtain a free copy of your credit report from each company listed below once every 12 months by requesting your report online at www.annualcreditreport.com, calling toll-free 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax	Experian	TransUnion
PO Box 740241	PO Box 9554	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
888-766-0008	888-397-3742	800-680-7289

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

As always, monitor your financial accounts closely and report any discrepancies.
Find more helpful information on identity theft and cybersecurity at www.ftc.gov.

Bayou Federal Credit Union 9-8-2017