



EQUIFAX

WHAT YOU NEED TO KNOW ABOUT THE 2017 EQUIFAX BREACH

This month, Equifax, one of the three major credit reporting bureaus, reported a massive data breach that left the information of 143 million people exposed.

Earlier this year, Equifax suffered one of the largest data breaches in history. It is reported that the data of 143 million people was left exposed for more than three months. It is still unclear what the hackers did with the data during this time. Events like this remind us that one of the most prevalent threats to today's consumer is identity theft. When hackers steal a consumer's identity, they often open bank accounts, apply for credit, and even file false tax returns using the victim's information. CUSA Federal Credit Union would like to address this event and give you vital information to help protect yourself.

First and foremost, take some time to ***make sure that all of your financial institutions have current contact information for you.*** This includes your home address, email address, cell phone number, and home phone number. Being able to contact you in the event that suspicious activity occurs is paramount in stopping identity thieves before things get out of hand.

Always ***open and review your account statements in a timely manner.*** Your diligence in monitoring balances and transactions is a powerful line of defense. Anytime you see suspicious information on your financial statements, please reach out to your financial institution immediately so that appropriate action can be taken.

Be aware that CUSA Federal Credit Union does have fraud monitoring protection policies in place, including member verification procedures. When CUSA reports your VISA credit card information to the credit bureaus, it only reports the last four digits of your credit card number. Also know that your VISA cards offer Zero Liability Protection so that you won't be held liable for unauthorized transactions. For more information on VISA's Zero Liability Protection, please visit www.visa.com.

Understand Phishing. In short, phishing is when a scammer tries to lure you into a trap by making fraudulent calls or sending fraudulent emails that attempt to solicit your personal information. Often times, the scammer will go through great lengths to be as authentic- looking as possible. Please remain vigilant and use caution when providing sensitive data. For more detailed information, please visit www.consumer.ftc.gov.

Consider placing a fraud alert on your credit. You can put a fraud alert on your credit reports for free by contacting one of the credit agencies, which is required to notify the other two. This means you'll be contacted if someone tries to apply for credit in your name. It will last for 90 days and can be renewed.

Review your credit report. Annualcreditreport.com will allow you one free credit report from Equifax, TransUnion, and Experian each year. You can then report any inaccurate or suspicious activity to the respective credit bureau.

For more information, please review the following links. Having the knowledge to combat the threat of identity theft could save you from the havoc that it can reap.

[5 Things to Do Right Now If You're Worried About the Equifax Hack](#)
[Equifax Data Breach: How to Freeze Your Credit](#)