



TechNEWS

Fall Edition!

Pittsburgh Computer Solutions 451 Valleybrook Road Suite 200 McMurray, PA 15317 724-942-1337



Equifax Data Breach



Among the Worst on Record

Equifax, which supplies credit information and other information services, reported on September 7th that a data breach could have potentially affected 143 million consumers in the United States.

The exposed data was discovered on July 29 which included names, birth dates, Social Security Numbers, addresses and some driver's license numbers, all of which Equifax aims to protect for its customers. For that alone, the breach ranks among the *worst* on record.

What happened?

According to Equifax the company's database was breached through a vulnerability on its website, exposing the personal information of an estimated 143 million people, including some in the UK and Canada.

What can you do?

It's possible by now many people already know what to do. A temporary credit freeze is a good place to start. It seems likely that many more people aren't doing much of anything, either because they don't know about the breach (Equifax is not emailing or even definitely confirming affected parties) or aren't sure whether taking action will actually have an impact.

So what are the consequences if you decide to do nothing at all? It's been strongly recommended to pull and read your credit report, followed by a credit freeze. These proactive steps certainly won't hurt you. Doing nothing potentially will.

Continued on pg. 2

The most likely thing that will happen is having your information misused in some manner, and end up needing to resolve that issue. There are a number of identity-theft cases where resolution can take up to anywhere from a couple of weeks to a couple of months, causing much distress and inconvenience.

The worst thing that could happen is that you ignore this problem and allow it to fester over time. You then have multiple identity-theft incidents across multiple silos that will take years to clean up. There is also the likelihood it will have some kind of negative impact on your life during a critical time, whether you're trying to get a job or purchase a home, get a car loan or a student loan.

While going through the process of trying to refinance their home, a couple notices things popping up on their credit report unfamiliar to them. If you choose to ignore the activity in the report, you'll find months down the road collection notices for credit cards that had been opened in your name. This type of scenario happens all of the time.

Millions of Americans have been impacted by the Equifax data breach. Whether or not your personal information has been compromised, these next 10 steps will help to protect yourself and your credit.



- 1. Review your credit report.** You are entitled to a free credit report every 12 months from each of the three major consumer reporting companies (Equifax, Experian and TransUnion). You can request a copy from AnnualCredit-Report.com.
- 2. Consider a security freeze.** A security freeze or credit freeze on your credit report restricts access to your credit file. Creditors typically won't offer you credit if they can't access your credit reporting file, so a freeze prevents you and others from opening new accounts in your name. In almost all states, a freeze lasts until you remove it. In some states, it expires after seven years.
- 3. Set up a fraud alert.** Fraud alerts require that a financial institution verifies your identity before opening a new account, issuing an additional card, or increasing the credit limit on an existing account. A fraud alert won't prevent lenders from opening new accounts in your name, but it will require that the lenders take additional identification verification steps to make sure that you're making the request. An initial fraud alert only lasts for 90 days, so you may want to watch for when to renew it. You can also set up an extended alert for identity theft victims, which is good for seven years.
- 4. Read your credit card and bank statements carefully.** Look closely for charges you did not make. Even a small charge can be a warning sign. Thieves sometimes will take a small amount from your checking account and then return to take much more if the small debit goes unnoticed.
- 5. Don't ignore bills from people you don't know.** A bill on an account you don't recognize may be an indication that someone else has opened an account in your name. Contact the creditor to find out.

6. Shred any documents with personal or sensitive information. Be sure to keep hard copies of financial information in a safe place and be sure to shred them before getting rid of them.

7. Change your passwords for all of your financial accounts and consider changing the passwords for your other accounts as well. Be sure to create strong passwords and do not use the same password for all accounts. Don't use information such as addresses and birthdays in your passwords. For more tips on how to create strong passwords contact PCS at 724-942-1337 and they will be able to assist you.

8. File your taxes as soon as you can. A scammer can use your Social Security Number to get a tax refund. You can try to prevent a scammer from using your tax information to file and steal your tax refund by making sure you file before they do. Be sure not to ignore any official letters from the IRS and reply as soon as possible. The IRS will contact you by mail. Don't provide any information or account numbers in response to calls or emails.

9. Active duty servicemembers are eligible for additional protections, and should also monitor their credit carefully. Learn more about what you can do if you're currently serving at home or abroad.

10. If you are the parent or guardian of a minor and you think your child's information has been compromised, you can go to the FTC (Federal Trade Commission) website and follow steps to protect their information from fraudulent use.



Don't get duped by phone scammers posing as Equifax



As if the Equifax data breach disclosing personal information for 143 million people wasn't enough, now scammers are taking advantage of the confusion and anxiety affecting customers. If you get a phone call from someone claiming to be part of Equifax, don't believe it.

Lisa Weintraub Schifferle, an attorney at the Federal Trade Commission, posted an article on the FTC's blog, alerting customers to the threat of deceitful phone calls from people claiming to be associated with Equifax. "Stop," wrote Schifferle. Don't tell them anything. They're not from Equifax. It's a scam. Equifax will not call you out of the blue."

Schifferle also offered tips and suggestions to avoid getting duped by scammers and imposters:


- Don't give personal information. Don't provide any personal or financial information unless you've initiated the call and it's to a phone number you know is correct.
- Don't trust caller ID. Scammers can spoof their numbers so it looks like they are calling from a particular company, even when they're not.
- If you get a robocall, hang up. Don't press 1 to speak to a live operator or any other key to take your number off the list. If you respond by pressing any number, it will probably just lead to more robocalls.

If you do get one of these calls, head to the Federal Trade Commission's Complaint Assistant page to report it.

Equifax is keeping consumers up to date as to the status of the data breach on its cybersecurity page. While you shouldn't expect a call from the credit bureau, you can always call Equifax yourself at 866-447-7559 if you have further questions or concerns.

Remember, if Someone Calls You From Equifax To Verify Your Account, It's A Scam!



A photograph of a brown glass growler with a metal clasp, a large metal key, and a crest on a wall. To the left is a window with a black frame. The wall is textured and aged. The text 'PCS Referral Program' is written in a cursive font in the upper right. Below the growler is a crest and the text 'PCS Knights'.

PCS Referral Program

It's simple to participate in the program. Send us a qualified referral (any business with 5 or more computers) and you'll receive a cool PCS Coat of Arms T-shirt!

When your referral books an appointment you will receive either a gift card valued at \$50, a beautiful gift basket full of goodies or even the awesome growler pictured on the left!

If your referral becomes a client you'll receive a monetary prize valued at \$100 or we will make a donation in your name to one of your favorite charities.

Unlock Your Rewards!

And that's not all...

Your name will be added to our Prize Wheel for a chance to win a grand prize with a value of \$500 or more! The spin will occur annually, held live via Facebook. For each new PCS client you are responsible for, the more chances you have to win!

To submit your referral: Call PCS at **724-942-1337**

Email: shaas@pcsmisp.com or ddeuerling@pcsmisp.com

Message us on Facebook *Be sure to Like us on Facebook!*