The Equifax Security Breach

The recent news that Equifax's database has been hacked has prompted phone calls and emails from concerned clients. We are writing to share some information with you about the break, Equifax's current course of action, and, most important, what you can do to protect yourself.
According to Equifax, the breach lasted from mid-May through July. Hackers targeted people's names, Social Security numbers, birth dates, addresses, driver's license numbers and credit card numbers were also stolen. This breach has affected 143 million people across the US, UK, and Canada.

Equifax will send correspondence by MAIL to those who were exposed. The company has put a tool on their website to check your potential impact and has made a free credit monitoring service available to those affected.

To find out if your information was exposed, click on the "Potential Impact" tab on the Equifax site and enter your last name and the last six digits of your Social Security number. Y*our Social Security number is sensitive information, so make sure you're on a secure computer and an encrypted network connection* any time you enter it. The site will tell you if you've been affected by this breach.

If your information has been compromised by the Equifax breach, it could be years before your data could be used illegally, so you must plan to be diligent for the long term. This includes reviewing your monthly bank and credit card statements along with your credit report for possible identity theft.

In the meantime, be wary of any emails you receive that are purportedly from Equifax and suggest you click on this or that link. The security breach is a perfect opportunity for fraudsters pretending to be from Equifax to prey upon the chance to steal your identity and/or compromise your computer's security. The best thing to do, always, when you receive an email from any business who asks you to click on their link is to instead find the company's website and follow any links you find there.

So what can you do now?

1. Check your credit report at annualcredtireport.com. Consumers are entitled to one credit report from each of the three reporting agencies each year. We recommend downloading a report from a different agency every three to four months.

- Download a report from Experian today, TransUnion in January, and Equifax in May to monitor your credit year-round without charge.

2. Stop pre-screened credit offers to limit future exposure by calling 888-5OPTOUT (888-567-8688).

- You can also opt out online.

3. Place a CREDIT FREEZE on your accounts. While a credit freeze does not prevent current creditors from accessing your credit report, it does restrict the ability of new creditors to access your

credit information. In other words, if you already have an account with Chase, an identity thief may still be able to open an account through Chase since that is not a "new" creditor.

- A credit freeze can temporarily be lifted and then put back in place if you are actively seeking credit.

4. Put a fraud alert on your files. A fraud alert warns creditors that you may be an identity theft victim. The creditor must then verify the identity of anyone seeking credit in your name before your credit information can be released.

- For detailed information about credit freezes and fraud alerts, click here.

5. Last, but not least, file your income taxes early each year and be sure to respond to any IRS correspondence immediately. Doing so will limit the ability of scammers to use your Social Security numbers to get a tax refund in your name.

- Scammers also use stolen Social Security numbers to apply for work, when arrested for crimes and infractions, to get medical care, and to steal benefits to which you are entitled.

If you discover that you are a victim of identity theft, visit identitytheft.gov to report and start your recovery plan immediately. Clients should also contact us so we can begin helping you with any necessary changes to your financial information.