There is a very good chance the Equifax Data Breach may have effected you. You would think with data breaches happening regularly that each of us would have something in place to monitor and protect. If you have not moved in the direction of using a service now is the time. There are many companies that provide the service.

This breach is significant and should be taken seriously. A weakness in Equifax's server security was hacked from mid-May through July, exposing names, addresses, social security numbers, birth dates and some driver's license numbers of millions.

To determine if you are effected Equifax has created an online registry to check. But, you should proceed as if you were hacked. It is safe to assume that if you have credit, you were breached.

Steps Recommend:

- Follow the link above to determine if you were effected, if yes, enroll in the monitoring system provided by Equifax. This will be provided for a year free after determining you are at risk. This monitors all bureaus, allows you to lock your Equifax credit report and provides a copy of your existing report to review. In addition, should your identity be stolen, they provide up to $1m in insurance.
- Second located and obtain services through an additional source. There are several companies that offer this service; Lifelock being one of the top in the industry.
- Next, if you have any credit cards that do not have a chip, it is recommended that they are replaced as soon as possible.
- Locking down credit is the next step. It is worth whatever few dollars it cost because the cost is incrementally less than identity theft. Freezing your credit with each of the bureaus blocks anyone from opening any kind of account with your credit. However, if you are in the market for a new home or new car or apply for a new credit card, you will need to then unfreeze your credit PRIOR to purchasing. Yes, it may cost $0 to $15 to freeze your credit at the bureau(s). In this case, it's worth it.
- If you do not want to freeze your accounts, put a fraud alert on your accounts. This will alert creditors to validate the identity of the one attempting to gain credit with your information. Typically, they will call the phone number to verify it is truly you. You can even get an extended fraud alert which is good for seven years.
- **File next year's tax return** as soon as allowed. Though this is a few months away, since they have your social security numbers, consider filing your tax return sooner than later. Start preparing now and then the end of year will not be nearly as chaotic.
- **Lastly, be aware of potential phishing emails** that will arise out of this breach. They will want to you click on a link to verify a credit card or a transaction or did you ask for new credit or blah blah blah.

  NEVER EVER click on a link in an email. NEVER EVER. The link may lead you to what looks like a valid site but it is not. ALWAYS validate the source and if you do not know how, do not do anything. Call the creditor's telephone number on the back of your credit card or on your statement if you are concerned. Consider all those types of emails invalid. Again, particularly vulnerable are our senior citizens. Have a conversation with yours about this breach and online security as well.

  We need to become diligent in protecting our credit information.