BARRETT
ASSET MANAGEMENT, LLC
SINCE 1937
90 Park Avenue • New York, NY 10016

Stop Thief, FREEZE!

In recent years, nary a financial institution or large retail establishment has avoided being hacked and having the private information of their customers stolen. The recent breach of data at Equifax, the Fort Knox of personal information, has resulted in the personal information of almost every American being left vulnerable.

What can you do to protect yourself and your data?

We highly recommend that you consider placing a **Security Freeze** on your credit file. This is the most effective way to thwart identify theft. We detail below what steps you can take to protect yourself and your family. Incidentally, Barrett Asset Management was consulted on this very topic by the New York Times and mentioned in this very informative article: https://nyti.ms/2xUP4Kb

A credit freeze seals your credit reports so no new credit applications can be initiated in your name without your knowledge. When you set up a credit freeze, you get a personal identification number that only you know. You can use it to "thaw" your credit when you need to. The freeze does not affect your existing lines. This is one step more than Credit Monitoring or Fraud Alert. Essentially, you make it so your data has no value because it cannot be used to open accounts in your name. This is the best line of defense against identity theft.

How to freeze your credit files:

You can freeze your credit files by logging on to the websites of the four credit reporting agencies:

- Experian https://www.experian.com/freeze
- TransUnion https://freeze.transunion.com
- Equifax https://www.freeze.equifax.com/Freeze
- Innovis https://www.innovis.com/personal/securityFreeze

You must freeze your files at all four agencies and it must be done for each member of the household. Even though these agencies may have been hacked, placing a freeze on your files will essentially create a moat around your data.

We will admit that it is not the easiest thing to do as there are many levels of security that you must go through to activate this feature at each agency. And whatever you do, DON'T misplace your security unlock PIN. However, we have assisted many clients in this process. Should you have any questions, we can help guide you through the procedure and answer any questions you may have about identity theft and the precautions that you can take. In the meantime, we encourage you to share this essay with your friends and family.

Christina Bater, CFP®
Managing Director and Wealth Planner
www.barrettasset.com
September 2017

HOW TO PROTECT YOURSELF FROM IDENTITY THEFT, CREDIT CARD FRAUD AND EMAIL HACKING

- Use a credit card vs a debit card as the protection levels are higher. You can even have your bank deactivate the debit card feature on your ATM card.
- Change your online banking password and debit card PIN.
- Carefully review your monthly checking and credit card statements. Reduce the number of credit card accounts you have so that you can adequately review the transactions at least once a month.
- Backup your data locally.
- Buy a shredder and use it.
- Change your passwords regularly and don't use the same password for all accounts.
- Be particularly vigilant with your email accounts. You may even want to implement a two-step login verification process.
- If you get an email that says it's from the IRS, do not click on any links in the email. Just delete it. If anyone contacts you by email or phone and says they're from the IRS, hang up. The IRS will only contact you via mail.
- Never provide anyone who has contacted you (via phone or email) with your Social Security number, date of birth, bank account information, passwords, etc. If you're worried about whether someone contacting you is legitimate, call the IRS at 800-829-1040.
- Keep your email boxes empty—this includes Sent and Deleted folders. Sometimes hacking can be very low tech. Prior emails may contain your account numbers or samples of your signature. Be sure to double delete sensitive emails after sending.
- Watch out for anything odd—a medical explanation of benefits for a service you didn't have. Even Medical Insurance is being stolen these days.
- Order an annual credit report even if your credit files are frozen.
- Stay informed on common scams and warning signs
    - https://www.identitytheft.gov/
    - https://www.usa.gov/online-safety#Learning_about_Internet_Fraud
    - https://www.irs.gov/identity-theft-fraud-scams
- Keep personal information confidential.
- Password protect your cell phone.
- Lastly, if you have been hacked or the victim of identity theft, REPORT IT!