Important Information on Identity Theft

Identity theft has been a serious threat to consumers for many years. The recent Equifax data breach has raised awareness due to the sheer magnitude of the incident which affected 143 million consumers nationwide. Other notable incidents with recognized consumer brands have included Yahoo (2013), Target (2013), eBay (2014), Home Depot (2014) and Anthem (2015).

Situations like the ones above are mostly outside of your control, as many consumers have done business with these companies. The Massachusetts Attorney General has provided information on how consumers can protect themselves from potential identity theft related to the Equifax breach. The information can be found here: http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-09-08-equifax-data-breach.html

In addition to these steps, we encourage clients to make the following a part of their routine to deter identity theft and unauthorized access to personal information:

1. ***Improve your passwords***. Create a strong password. Consider using a combination of capital letters, numbers and punctuation marks. Even if your "base" password is easy for you to remember, adding in the other characters will strengthen it and protect from hackers. You should also ***consider enabling two-factor identification*** on sites that offer this feature. Two-factor ID requires entering an additional code, provided via text or email, to access specific sites.
2. ***Consider using a password manager*** for storing the many passwords we accumulate in today's digital age. The password manager is opened by one master password and all others are then stored for you to access and update. There are many password managers that offer this protection, including: LastPass, KeePass, 1Password, and Dashlane.
3. ***Never open links, files, or documents received via email from an unknown sender***. Delete that email - if it's important, the sender will contact you again and you can have them resend it once you know more. Also, always check the sender's email address to make sure the address itself is familiar.
4. ***Check your credit report every 4-6 months.*** As the information from the Attorney General recommends, go to https://annualcreditreport.com to get a free credit report. If you notice an account or activity that is not familiar to you, call the company directly to clarify the entry on your report.
5. ***Take immediate action if you suspect identity theft.*** If you notice suspicious activity, the Federal Trade Commission has a website to deal with identity theft, https://identitytheft.gov. Here are some signs, provided by the FTC, that someone may have stolen your identity:
    - Unexplained withdrawals from your bank account.
    - You don't receive expected bills / notice mail which may have been redirected.
    - Unfamiliar accounts or charges on your credit report.
    - Merchants refuse your checks or transactions.
    - Debt collectors call you about debts that aren't yours.
    - Medical providers bill you for services you didn't use.
    - Health plan rejects a legitimate claim because records show you've reached your benefits limit.
    - Health plan won't cover you because your medical records show a condition you don't have.
    - The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.
    - You get notice that your information was compromised by a data breach at a company where you do business or have an account.

Protecting financial data and personal information is a burden that has increasingly been placed in the hands of individuals. We encourage you to take an active role in protecting yourself and your family. Please feel free to call if you have any questions.