As a follow-up to our personal note in the spring, "Developing Your Family's IT Security Plan," we are doing a more in-depth look at some potential threats that are employed by nefarious individuals looking to either exploit or steal our personal information for monetary gain leading up to our annual tax preparation.

As tax season rapidly approaches, our industry always sees a spike in illegal activity that looks to take advantage of individuals who may be more vulnerable and can pose an immediate threat to our personal information.

While we cannot insulate you from these attempts, we feel that having adequate knowledge about these potential scenarios will help you to respond in a way that can disarm the attempt and allow you to take proactive steps to prevent the fraud from taking place.

Remember, it is not a matter of **"if"** you will be impacted, but **"when"** and **"how**,**"** so it is critical to be able to identify a potential attempt to compromise your information and how to effectively respond.

The Internal Revenue Service (IRS) recently published a list of the threats to consumers related to the IRS and here are the top five:

1. **Identity Theft:** If you've been a victim of stolen personal information, contact the IRS at www.irs.gov so the agency can work to prevent the filing of fraudulent tax returns and refund claims in your name.
2. **Phishing:** Be wary of fake emails or websites looking to steal your personal information. If you receive a request for information that appears to be from the IRS, contact the IRS directly to verify the request.
3. **Telephone & Email Scams:** Scammers impersonating the IRS may say you are due a large refund or owe money (and may even make threats). Report the call or email immediately to the IRS and the Federal Trade Commission using their "FTC Complaint Assistant" at www.ftc.gov. The IRS provides official notices via regular mail only.
4. **Tax Return Preparer Fraud:** Dishonest preparers may use tax preparation as an excuse to steal your personal information or file false returns with big refunds payable to them. Only use a preparer who signs the return and has an IRS Preparer Tax Identification Number.
5. **Impersonation of Charitable Organizations:** Donate only to recognized charities and beware of charities whose names sound similar to the well-known ones. You can determine if a charitable organization is a legitimate one at the following websites: www.charitynavigator.org, www.charitywatch.org and www.givewell.org.

To help our clients better understand how these threats can impact them, we asked our strategic partner for tax preparation, Lisa Schorr, to share some experiences that she has encountered during her tenure.

Lisa Schorr has been a strategic tax partner to our practice for over thirty years and has been an invaluable resource for our clients when it comes to tax preparation and outlining how tax liabilities can impact your investment strategy and retirement plan.

1. Lisa, could you share with us an example of fraud that you see on a regular basis?

Many of us have received a call from someone identifying themselves as a representative from the Internal Revenue Service. Generally, the caller has a foreign accent and states that there is an outstanding balance due on your taxes and that a law enforcement is on his way to your home to take you into custody. Such callers prey upon fears that you, as the taxpayer, will incur significant penalties and land in jail. The scam artists use phone calls, leave messages on your machines and send e-mails either declaring you have an unexpected tax due which needs to be paid immediately, or they promise a refund and need your bank information to deposit the refund into your account.

2. Any new threats that you have heard about recently that may not be as prevalent in the media?

One tactic involved advising taxpayers to pay their taxes using an iTunes gift card from Apple. Most recently, a new scheme has emerged that targets students and their parents warning that they have not paid their "Federal Student Tax" and that any student loans and college acceptance may be in jeopardy if this tax is not paid immediately. Some scammers alter caller ID numbers to make it appear that the call is from the IRS or another agency. Communications are generally done with poor grammar, misspellings and inaccurate identification, such as "Internal Revenue Agency" as opposed to "Internal Revenue Service," "Federal Student Tax" when there is no such tax, etc. Regardless of how these the scams sound, taxpayers have paid millions of dollars to scammers in fear of problems with the IRS. The iTunes scam alone resulted in over $1.4 million in gift cards sent to scammers by over 300 individuals.

3. What can our clients do when they are posed with these types of threats and how do we differentiate what is real and what is not?

It is important to do your due diligence; the nefarious individuals are trying to create fear and hope that it will force you to turn over control of your personal information to them. It can happen quickly or slowly over time, but the best way to disarm these threats is through knowledge. Remember that the IRS ALWAYS initiates contact with taxpayers through written correspondence, providing for 30 days to respond. Keep the following points in mind when it comes to scammers and their common tactics:

1. *Call taxpayers or send an e-mail requesting verification of taxpayer identity by asking for personal and financial information.*
2. *Demand immediate payment of a tax due without allowing time for the taxpayer to respond to their assessment.*

3. *Threaten to bring federal, state or local police to arrest a taxpayer for not paying an unsettled tax burden.*
4. *Require that taxpayers use a certain form of payment to satisfy a tax liability.*
5. *Ask for credit or debit card numbers over the phone or by e-mail.*

4. If you are a subject of these threats, what can you do to be proactive?

1. *Do not give out any information.*
2. *Do not click on any attachments or links to any questionable e-mails claiming to be from the Internal Revenue Service or other governmental agency.*
3. *Call the IRS directly at 800-829-1040 to determine if you owe any taxes.*
4. *Contact the Treasury Inspector General for Tax Administration (TIGTA) at 800-366-4484 to report the call, or go to their web page (IRS Impersonation Scam Reporting) using the following link to report the scam:* https://www.treasury.gov/tigta/contact_report_scam.shtml
5. *You can also report the scam to the Federal Trade Commission using the following link:* https://www.ftccomplaintassistant.gov/#&panel1-1 *and include "IRS Telephone Scam" in the application notes.*

5. **Lisa, is there anything else you want to share with us about these potential threats?**

Yes, when in doubt, you must take control and figure it out. You must have a plan and it needs to be updated regularly. Do not leave anything to chance, because it can take years to repair the damage once your personal information is compromised.

Again, our goal is to always try to help our clients see things that could impact their plans and the threat to our personal information has never been greater. We strongly recommend that you take this quiz to assess your readiness (Test Your Cybersecurity IQ) and use this guide (A Bank Customer Guide to Cybersecurity) as a starting point to develop an information security plan for you and your family, and continue to update it regularly. Our team feels that the development of this plan is critical and if you ignore the risks, it is only a matter of time before your information or assets will be compromised due to fraud and theft.

We hope you continue to find these series helpful and a big thank you to Lisa Schorr for her contribution and the value she has brought to our clients over the past thirty years. Our practice continues to be extremely fortunate to have great partners, such as Lisa, who help us grow our expertise in areas that are critical to our clients' Investment and Retirement Planning process.

In addition to this monthly topic, please watch for our market updates that will be coming out in the next few weeks.

Please do not hesitate to contact us at 412-823-4704 if you have any questions or would like to schedule a review.

As we continue to move towards the latter part of 2016, we wish you and your families continued health and prosperity.

Thank you,

CFG Team