

FINANCIAL SECURITY PLANNING SERVICES, INC.SM



Market Thoughts & Tax Identity Theft

April 2018

[Join Our Mailing List!](#)

[Forward to a Friend](#)

Market Thoughts for April 2018

Brad McMillan, Commonwealth's Chief Investment Officer, recaps the market and economic news for March. Last month, both U.S. and international markets saw losses. It was the second down month in a row, something we haven't seen in a while. This was due, in part, to markets becoming uncertain on the news of tariffs on China-which rattled companies around the world. Plus, Fed Chair Powell was seen as more hawkish than expected, introducing uncertainty around interest rates. Despite all this, do the fundamentals remain solid? Tune-in to find out.



We hope you enjoy this month's video.

What Should You Do if You Are a Victim of Tax Identity Theft?

When it comes to filing your tax return, you put in the time and effort to complete every form accurately and according to the instructions. But even if

you do everything by the book, a tax identity thief may still file a fraudulent return in your name. Unfortunately, this happens all too often. In fact, despite having prevented more than 787,000 fraudulent tax returns in 2016, the Internal Revenue Service (IRS) paid out \$239 million in "suspect" refunds.

So, what steps should you take if you find yourself a victim of tax identity theft? To help answer this question, let's take a look at how cyber criminals obtain your personal information.

How does tax identity theft work?

Cyber criminals can obtain your personal information in a number of ways, including the following:

- Posing as an IRS representative and procuring information via phone or e-mail
- Sending phishing e-mails
- Stealing your W-2 from your mailbox
- Accessing personal information over nonsecure Wi-Fi networks

To fraudulently file taxes, a thief needs your name, Social Security number (SSN), and date of birth. From there, he or she can easily falsify "your" W-2 information in the hopes of claiming a refund. You-the taxpayer-won't find out about the fraud until you receive notification from the IRS that your real tax return has been rejected. By then, the damage has already been done.

Now what?

Once your SSN has been compromised, it cannot be canceled or changed. But what you can do? Take the following steps to protect yourself from the fraudulent use of your SSN going forward.

Notify the Federal Trade Commission (FTC), Social Security Administration (SSA), and IRS. The faster you take action, the better! In addition to filing a complaint with the FTC and notifying the SSA, be sure to call the IRS Identity Protection Specialized Unit at 800.908.4490 to report the theft.

Submit IRS Form 14039. If you haven't already done so, submit IRS Form 14039 (i.e., the Identify Theft Affidavit), so that the IRS is aware that your future returns may be at risk.

Apply for an Identity Protection PIN. Once you've been identified by the IRS as an identity theft victim, you can apply for an Identity Protection PIN. This six-digit PIN, provided by the IRS, must be used for your future tax returns in order for them to be accepted.

Report the fraud to a major credit bureau. Report the fraud to one of the three major credit bureaus (Experian, TransUnion, or Equifax), and place an alert on your credit report. When you file a report with one bureau, it is legally required to alert the other two. A fraud alert on your credit report will require

potential creditors or lenders to contact you directly and obtain permission before opening a new line of credit.

Consider purchasing credit monitoring. With credit monitoring, you'll be able to keep tabs on your credit report. Credit monitoring services will alert you when a new line of credit is attempted, but they will also monitor existing accounts and notify you of any changes. Many also offer recovery assistance services, monetary and legal assistance, and insurance that covers expert consulting regarding identity theft.

Stay aware!

Your situation may run its course and go away for a couple of years. Unfortunately, you are likely to have another issue considering that your SSN is in the hands of at least one identity thief. As such, you must always stay aware.

As mentioned earlier, credit monitoring can help you keep tabs on your credit. You may also want to file your taxes as soon as possible each year to avoid another fraudulent filing. Finally, remember that the IRS will never contact you electronically and almost never over the phone. It always communicates via letters through the U.S. Postal Service. If you do receive a phone call from someone saying that he or she is from the IRS, hang up and call your local IRS office directly.

My staff and I deeply appreciate the continuing opportunity to work with you. Please let me know if you have any questions or requests. Thank you.

Sincerely,

Paul S. Bonapart, JD, RFC, AIF®, President
Financial Security Planning Services, Inc.
520 Tamalpais Dr, Suites 103 & 104
Corte Madera, CA 94925
(415) 927-2555
www.FinancialSecurityPlanning.com
CA Insurance License No. 0808412

- Registered Representative with/and offers securities through Commonwealth Financial Network, member FINRA/SIPC, a Registered Investment Advisor.
- Advisory services offered through Financial Security Planning Services, Inc. a Registered Investment Advisor, are separate and unrelated to Commonwealth Financial Network.
- Fixed insurance products and services offered through CES Insurance Agency.
- Indices are unmanaged and cannot be invested into directly. Past performance is not indicative of future results.
- This material has been provided for general informational purposes only and does not constitute either tax or legal advice. Although we go to great lengths to make sure our information is accurate and useful, we recommend you consult a tax preparer, professional tax advisor or lawyer.

- © 2018 Commonwealth Financial Network®

Delivering financial confidence since 1992

