

# Protecting Yourself From Tax Identity Fraud

Wealth Management Insights | January 2017

*Tax identity fraud commonly refers to the practice of using a stolen Social Security number to file a false tax return and claim a fraudulent refund. This scam costs taxpayers billions of dollars per year and can ruin its victims' finances and credit rating. This month's Wealth Management Insights looks at what you can do to protect yourself from this kind of fraud.*

.....  
For more tips on staying cyber-secure, check out our [Wealth Management Insights brief on safe shopping](#), featuring the insights of retired FBI special agent Jeff Lanza.  
.....

## What you should know:

- 1. Protecting physical documentation is essential.**
  - Monitor your bank and credit card statements. If you don't regularly reconcile each purchase, at least make sure the merchants listed on each statement are ones you have visited.
  - Safeguard your Social Security card, all tax documents and all bank and credit card receipts. File what you need and shred what you don't.
  - Update your employer, financial institutions and the Internal Revenue Service each time you move. Having tax documents mailed to an old address opens the door to tax identity theft.
- 2. Consider what information you're making available online.**
  - Any information you enter – like usernames and passwords – on public Wi-Fi can be easily intercepted. Don't reuse passwords and save sensitive financial transactions like electronic banking or tax return filing for when you're on a secure, private connection.
  - While you once could identify email scams from spelling and other language errors, criminals have become more sophisticated over time. If you're unsure of the validity of a request or are being pressured to act immediately, contact the institution offline. ▶

- Safeguard your Social Security number. If con artists can link up a name with a Social Security number, they have enough information to file a fraudulent tax return. Remember, most legitimate financial institutions will not ask for your Social Security number online or over the phone.

### 3. Know when you're being scammed.

- Be wary of anyone contacting you over the phone or by email claiming to be from the IRS. The IRS will never initiate contact with you via telephone or email – only by letter.
- If the IRS receives two electronic returns for the same Social Security number, it will reject the second one. Filing your return promptly can thwart would-be thieves.

- If the IRS notifies you of a second return filed on your behalf or a discrepancy in your earned wages, it can pay to respond quickly. Contact the IRS Identity Protection Specialized Unit and the three major credit reporting bureaus (Equifax, Experian and TransUnion) regarding potential fraudulent activity.

### What you should do now:

While the potential for tax identity fraud can never be eliminated, following a few common-sense guidelines can dramatically reduce your likelihood of becoming a victim. **Your Baird Financial Advisor** has additional insight into how you can keep your finances and identity safe in an increasingly online world. ■