

Tax Season Scam Alert

Presented by Steven E. Richardson, CFP®, CRPS®, President

With tax season upon us, many of us are busy gathering the appropriate documents, meeting with CPAs, and ensuring that relevant tax deadlines are met. But in all the hustle and bustle, taxpayers also need to keep an eye on the risks, especially tax season scams. Each year, scammers get more savvy with strategies they use to gain access to other people's personal information and money. To help you steer clear of this year's top scams, learn red flags to watch out for—along with some timely tax-filing reminders.

“Ghost” Tax Return Preparers

One truly frightening scam haunting taxpayers is the ghost preparer. These preparers remain hidden from the IRS by not signing returns, making the returns appear to be self-prepared. In cases where the individual e-files, the ghost preparer will refuse to digitally sign the return. The result can be disastrous for taxpayers, leaving them open to serious filing mistakes, tax fraud, penalties, and audit by the IRS.

Red flags. To help avoid this issue, be in the know when it comes to red flags surrounding ghost preparers. They usually:

- Don't sign the return with a Preparer Tax Identification Number (PTIN) (The PTIN is required by law for anyone who is paid to prepare or assist in preparing a federal tax return.)
- Lure clients in with the promise of big refunds (Unfortunately, these scammers will resort to claiming fake deductions to boost the size of the refund.)
- Require payment in cash
- Have refunds directed into their bank accounts, not the taxpayer's

Pro tip. If you're looking for someone to prepare your taxes, the IRS has a [great online resource](#) that offers a tool for checking your tax preparer's credentials and tips for avoiding potential tax scammers. No matter who prepares your return, it's important to review it carefully, including the routing and banking numbers if you're receiving your refund via direct deposit.

New Round of COVID-19 Scams

As the coronavirus continues to spread, so do scams, unfortunately. Criminals often try to exploit taxpayers during times of uncertainty, and this pandemic has been no exception. The latest COVID-19 scams center around the most recent round of stimulus payments. They have taken on a few forms, all with the singular goal of stealing taxpayers' money and personal information.

Red flags. The IRS Criminal Investigation division has compiled a list of the latest COVID-19 scams. Here's what to be on the lookout for:

- Text messages asking you to disclose bank account information in order to receive the \$1,200 economic stimulus
- Emails, letters, and social media messages that use “coronavirus,” “COVID-19,” and “stimulus” in different ways, requesting personal information and financial account information (e.g., account numbers and passwords)
- Sale of fake at-home COVID-19 test kits
- Fake donation requests for individuals, groups, and areas heavily affected by COVID-19
- “Opportunities” to invest in companies developing COVID-19 vaccines, which also promise these companies will drastically increase in value as a result

Pro tip. If you receive unsolicited emails or social media attempts that are aimed at gathering your personal information and appear to be from the IRS or an organization linked to the IRS, forward the message to phishing@irs.gov.

Online Identity Theft

One of the most common tax scams remains personal identity theft, which is particularly rampant during tax season. Why? By accessing the social security numbers, addresses, and birth dates of unsuspecting taxpayers, scammers can file phony tax returns and steal refunds. The worst part is this can all be done before the victims even know their identities have been stolen.

Red flags. So, what can you do to help ensure that someone doesn't file a return in your name? Know the warning signs of this pervasive scam:

- If you receive an IRS notice regarding a duplicate return, that you received wages from somewhere you never worked, additional taxes are owed, the refund will be offset, or collection actions are being taken against you for a year you did not file a tax return, contact the IRS *immediately*.
- As noted above, ensure that your tax preparer has the appropriate credentials.
- Unless there is a valid reason, don't give out your social security number—and always know who you're giving it to.

Pro tip. The best way to avoid this scam is to file your taxes early, before a scammer can access your information. You might also think about using an [Identity Protection PIN](#) (IP PIN) to proactively protect yourself from identity theft. The IP PIN is a six-digit number known only to you and the IRS that can be used to help the IRS verify your identity when a paper or electronic tax return is filed.

Never Has the IRS Ever . . .

When it comes to tax scams, one of the most important things to know is how the IRS does (and *doesn't*) contact taxpayers. Here are some things the [IRS](#) just won't do:

- Demand that you pay taxes without the opportunity to question or appeal the amount it says you owe
- Call to demand you make an immediate payment using a specific method (e.g., prepaid debit card, gift card, or wire transfer)
- Threaten to bring in local police, immigration officers, or other law enforcement to arrest you for not paying (Threats are a common tactic used by scammers.)

So, if you get a call or email that sounds like any of the above, it's likely a scam. For steps to take if you suspect fraudulent tax activity, visit the IRS's [Report Phishing and Online Scams page](#).

Scams Don't End with Tax Season

Although the focus here is on tax season, we would all be wise to remember that new scams are popping up every day, year-round. So, remain vigilant in keeping your personal information safe and be on the lookout for potential scams.

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.

###

Steven E. Richardson, CFP®, CRPS®, President is located at Potomac Financial Private Client Group, LLC, 11130 Sunrise Valley Drive, Suite 130, Reston, VA 20191 and can be reached at 703.891.9960 The financial consultants of Potomac Financial Private Client Group, LLC are Registered Representatives with/and offer securities and advisory services through Commonwealth Financial Network, Member FINRA/SIPC, a Registered Investment Adviser. Fixed insurance products and services offered through CES Insurance Agency.