Key Private Bank

Filer Beware:

July 9, 2021

The Top Tax Scams of 2021

Tina A. Myers, CPA , CFP, CPA/PFS, MTax, AEP , Director of Financial Planning

Several years ago, the IRS began to compile an annual list of common tax scams known as the "Dirty Dozen." Each of the scams that makes the list was highlighted by the IRS with an announcement over twelve consecutive days to raise awareness.

This year's "Dirty Dozen" list was issued over four days instead of twelve, with each scheme placed in one of four categories based upon who perpetuates the schemes and who they impact: The separate categories are:

- **Pandemic-related scams** like Economic Impact Payment theft.
- **Personal information cons** including phishing, ransomware, and phone "vishing."
- **Ruses focusing on unsuspecting victims** like seniors/immigrants and using fake charities.
- **Schemes that persuade taxpayers into unscrupulous actions** such as Offer In Compromise "mills" and syndicated conservation easements.

The IRS urges all taxpayers to be on guard, especially during the pandemic, not only for themselves but also for other people in their lives.

Check out this year's "Dirty Dozen" tax scams:

Pandemic-related scams

Economic Impact Payment theft: Identity thieves try to steal Economic Impact Payments (EIPs), also known as stimulus payments. Most eligible people get their payments automatically from the IRS. Taxpayers should watch out for stimulus check scams. The IRS won't initiate contact by phone, email, text, or social media asking for Social Security numbers or other personal or financial information related to Economic Impact Payments.

Remember: The IRS website, IRS.gov, is the agency's official website for information on payments, refunds, and other tax information.

Unemployment fraud leading to inaccurate taxpayer 1099-Gs: Scammers took advantage during the pandemic to file fraudulent claims for unemployment compensation using stolen personal information of individuals who had not filed claims. Payments made on these fraudulent claims went to the identity thieves. Look out for receiving a Form 1099-G reporting unemployment compensation that a taxpayer didn't receive.

Personal information cons

Tax-related phishing scams persist: Be alert for a continuing surge of fake emails, text messages, websites, and social media attempts to steal personal information. These attacks tend to increase during tax season and remain a major cause of identity theft throughout the year. Cybercriminals usually send these phishing communications by email but may also use text messages or social media posts or messaging. Taxpayers are reminded to continually watch out for emails and other scams posing as the IRS, like those promising a big refund/missing stimulus payment or even issuing a threat. People should not open attachments or click on links in those emails or text messages.

Phishing scams targeting tax professionals. The IRS warns tax professionals about phishing scams involving verification of Electronic Filing Identification Numbers (EFIN) and Centralized Authorization File (CAF) numbers.

The agency has seen an increase in these kinds of scams, along with offers to buy and sell EFINs and CAFs.

Phishing – new client scams target tax pros. The "New Client" scam continues to be a prevalent form of phishing for tax pros. Here's an example in the form of an email: "I just moved here from Michigan. I have an urgent tax issue and I was hoping you could help," the email begins. "I hope you are taking on new clients." The email says one attachment is an IRS notice and the other attachment is the prospective client's prior-year tax return. Tax professionals should be wary and avoid opening attachments or clicking links when they don't know the email sender.

Impersonator phone calls/vishing. Individuals should be wary of unexpected phone calls asking for personal financial information. The IRS has seen an increase in voice-related phishing, or vishing, particularly from scams related to federal tax liens. For those receiving phone calls out of the blue, ask questions and if in doubt, hang up immediately.

During 2020, almost 400 vishing scams were reported, a 14% increase from the prior year. Of those vishing scams, 25% were scammers who tried to use fake tax-lien information. The number of tax-lien related scams increased from 58 in 2019 to 104 in 2020, an increase of 79%. The IRS urges taxpayers to refrain from engaging potential scammers on the phone or online.

While both the IRS and the Federal Trade Commission have seen a decline in the number of reports of scammers claiming to be from the IRS telephoning potential victims, the agency urges taxpayers to be wary. The IRS has seen a 43% decrease in the number of reports of calls from callers claiming to be from the IRS: 20,500 in 2020 compared to 36,000 in 2019. The FTC reported a 67% decline from 7,694 reports in 2019 to 2,571 in 2020.

Social media scams continue. Social media enables unscrupulous individuals to extract personal information to use against the victim. These cons may send emails impersonating the victim's family, friends, or co-workers. Social media scams have also led to tax-related identity theft. A scammer may email a potential victim and include a link to something of interest to the recipient but that contains malware intended to commit more crimes. Scammers also infiltrate their victim's emails and cell phones to go after their friends and family with fake emails that appear to be real and text messages soliciting, for example, small donations to fake charities that may appeal to the victims.

Ransomware on the rise. Ransomware is a form of malicious software ("malware") designed to block access to data or programs on information technology (IT) systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data.

The US Treasury Financial Crimes Enforcement Network (FINCEN) has noted that ransomware attacks continue to rise across various sectors, particularly governmental entities as well as financial, educational and healthcare institutions. This is likely due to the victims' weaker cybersecurity controls, such as inadequate system backups and ineffective incident response capabilities.

Ransomware actors are increasingly engaging in selective targeting of larger enterprises to demand bigger payouts and sharing resources to enhance the effectiveness of ransomware attacks, such as ransomware exploit-kits that come with ready-made malicious codes and tools. Some ransomware groups are also forming partnerships to share advice, code, trends, techniques, and illegally obtained information over shared platforms.

Ruses focusing on unsuspecting victims

Fake charities. Be on the lookout for scammers who set up fake organizations to take advantage of the public's generosity, especially in times of tragedies and disasters such as the COVID-19 pandemic. Always research a charity before donating and don't feel pressured to donate immediately. A legitimate charity will be happy to get a donation at any time. Do not pay by giving numbers from a gift card or wiring money: Pay by credit card or check.

Immigrant/senior fraud. IRS impersonation scams remain common. This occurs when a taxpayer receives a telephone call threatening jail time, deportation, or revocation of a driver's license from someone claiming to be with the IRS. These scams target groups with limited English proficiency as well as senior citizens.

Offers in Compromise mills. Promoters mislead people with claims about settling their tax debts while charging excessive fees. Some promoters inappropriately advise taxpayers to file an Offer in Compromise application with the IRS, even though the promoters know the person won't qualify. Companies advertising on TV or radio frequently can't do anything for taxpayers that they can't do for themselves by contacting the IRS directly.

Unscrupulous tax return preparers. Although most tax preparers are ethical and trustworthy, taxpayers should be wary of preparers who won't sign the tax returns they prepare. Paid preparers must sign and include their Preparer Tax Identification Number (PTIN) on the return. Not signing a return is a red flag that the paid preparer may be looking to make a quick profit by promising a big refund or charging fees based on the size of the refund. Unscrupulous preparers may require payment in cash only, invent income to qualify for tax credits, claim fake deductions, and direct taxpayer refunds into their bank account, not the taxpayer's account. Taxpayers should choose their tax preparer wisely.

Unemployment insurance fraud. Unemployment fraud often involves individuals acting in coordination with or against employers and financial institutions to get state and local assistance to which they are not entitled. States, employers, and financial institutions should be aware of the following scams: identity-related fraud in submitting applications, employer-related collusion fraud, misrepresentation of income fraud, fictitious employer-employee fraud, and insider fraud where state employees inappropriately change unemployment claims.

Schemes peddled by tax promoters

Syndicated conservation easements. In syndicated conservation easements promoters take a provision of tax law for conservation easements and abuse it through using inflated appraisals of undeveloped land and partnerships. These arrangements are designed to game the system and generate inflated and unwarranted tax deductions, often by using inflated appraisals of undeveloped land and partnerships devoid of a legitimate business purpose.

Abusive micro-captive arrangements. Promoters persuade owners of closely held entities to participate in schemes that lack the true attributes of insurance. Coverages may "insure" implausible risks, fail to match genuine business needs, or duplicate the taxpayer's commercial coverages. Premiums paid under these arrangements are often excessive.

Potentially abusive use of the US-Malta tax treaty. Some US citizens and residents are relying on an interpretation of the US-Malta Income Tax Treaty (Treaty) to take the position that they may contribute appreciated property tax free to certain Maltese pension plans and that there are also no tax consequences when the plan sells the assets and distributes proceeds to the US taxpayer.

The IRS is undergoing an evaluation to determine the validity of these arrangements and whether Treaty benefits should be available in such instances; it may challenge the associated tax treatment.

Improper claims of business credits. Improper claims for the research and experimentation credit generally involve failures to participate in, or substantiate, qualified research activities and/or satisfy the requirements related to qualified research expenses. Taxpayers should carefully review reports or studies to ensure they accurately reflect the taxpayer's activities.

Improper monetized installment sales. Promoters find taxpayers seeking to defer the recognition of gain upon the sale of appreciated property and organize an abusive shelter by selling them monetized installment sales. These transactions occur when an intermediary purchases appreciated property from a seller in exchange for an installment note, which typically provides for payments of interest only, with the principal being paid at the end of the term. In these arrangements, the seller gets the lion's share of the proceeds but improperly delays the gain recognition on the appreciated property until the final payment on the installment note, often slated for many years later.

To fight the evolving variety of these abusive arrangements by tax promoters, the IRS recently created the Office of Promoter Investigations (OPI) to focus on participants and the promoters of abusive tax avoidance transactions. OPI coordinates service-wide enforcement activities.

The Top Tax Scams of 2021

Taxpayers are encouraged to review the "Dirty Dozen" list and be alert to these scams during tax filing season and throughout the year.

Protect Yourself: Security Reminders for Taxpayers: Do what you can to protect yourself. Here are some basic security steps to protect yourself and your sensitive tax and personal information:

Use security software. Always use security software with firewall and anti-virus protections. Make sure the security software is always turned on and can automatically update. Encrypt sensitive files such as tax records stored on the computer and use strong passwords.

Watch out for scams. Learn to recognize and avoid phishing emails, threatening phone calls, and texts from thieves posing as legitimate organizations such as banks, credit card companies, and government organizations, including the IRS. Do not click on links or download attachments from unknown or suspicious emails.

Protect personal data. Don't routinely carry a Social Security card, and make sure tax records are secure. Treat personal information like cash: Don't leave it lying around.

Work with financial institutions that have implemented processes to protect your private, banking, and financial information (such as multi-factor authentication, call-back verification for certain transactions, and email encryption programs to secure sensitive personal information). Multi-factor authentication allows users to better protect online accounts. One way this is accomplished is by requiring a security code sent to a mobile phone in addition to the username and password used to access the account.

Choose return preparers carefully. Avoid fly-by-night preparers. Ask if the preparer has an IRS Preparer Tax Identification Number (PTIN). Inquire whether the tax return preparer has a professional credential (enrolled agent, certified public accountant, or attorney).

Check preparer's qualifications. Use the IRS Directory of Federal Tax Return Preparers with Credentials and Select Qualification available on the IRS website to search for a tax preparer listed with the IRS.

Be wary of charities with names that are similar to familiar or nationally known organizations. IRS.gov has a search feature called Exempt Organizations Select Check that allows people to find legitimate, qualified charities to which donations may be tax-deductible.

Don't give out personal financial information such as Social Security numbers or passwords to anyone who solicits a charitable contribution.

Use IP PINs. The IRS made its Identity Protection PIN program available to all taxpayers this year. Previously, it was available only to victims of ID theft or taxpayers in certain states. The IP PIN is a six-digit code known only to the taxpayer and to the IRS. It helps prevent identity thieves from filing fraudulent tax returns using a taxpayer's personally identifiable information. Using an IP PIN is, in essence, a way to lock a tax account. The IP PIN serves as the key to opening that account. Electronic returns that do not contain the correct IP PIN will be rejected and paper returns will go through additional scrutiny for fraud.

Check privacy setting on social media. One way to circumvent these scams via social media is to review privacy settings and limit data that is publicly shared.

Practice good cyber hygiene. Practice proactive prevention to defend against ransomware attacks through effective cyber hygiene, cybersecurity controls, and other best practices.

Key Private Bank

Publish Date: July 9, 2021.
Source: IRS.gov