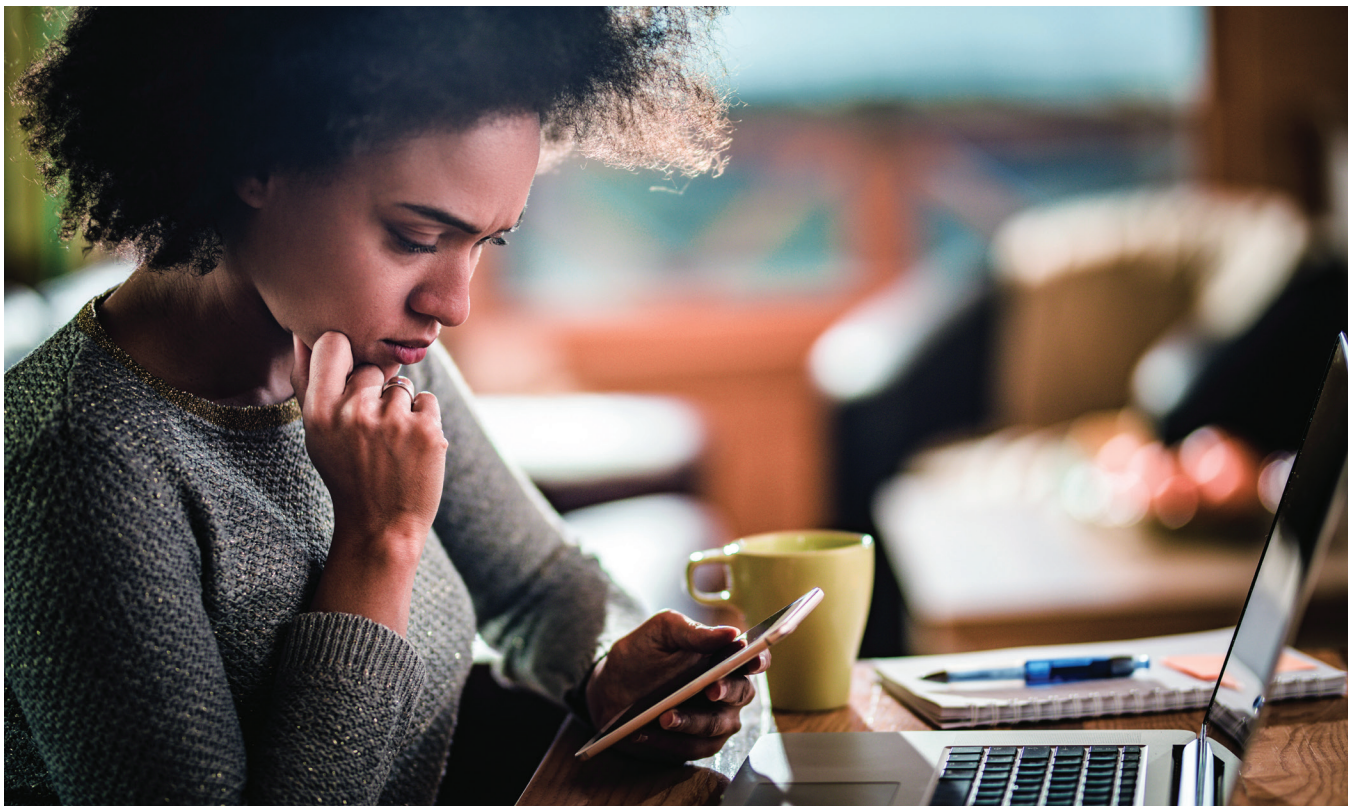
Key Wealth

Key Wealth Institute

IRS Releases Its Dirty Dozen Tax Scams and Schemes for 2024

Paul Kieffer, CPA/PFS, CFP®, Senior Wealth Planner



The IRS has compiled its annual list of common tax scams to remind taxpayers to use caution during tax season. The list is designed to protect taxpayers from potentially abusive arrangements, ranging from preparer fraud and identity theft to bogus tax maneuvers. These schemes put people at financial risk (including penalties and interest) and increase the chances that they could become victims of identity theft.

All the topics are repeats from last year, but many have updates for this year. The list is not a legal document nor a formal listing of agency enforcement priorities. It is intended to alert taxpayers and the tax professional community about various scams and schemes. Taxpayers are encouraged to review the Dirty Dozen list and stay alert to these scams during tax-filing season and throughout the year.

Phish or smish: Avoid getting hooked by either

Be alert to fake communications posing as legitimate tax or financial organizations, including the IRS and states.

- **Phishing** is an email sent by fraudsters claiming to come from the IRS or another legitimate organization, including state tax organizations or a financial firm. The email lures the victims into the scam by a variety of ruses, such as offering phony tax refunds or frightening people with false charges for tax fraud.
- **Smishing** is a text or smartphone message that uses the same technique as phishing. Scammers often use alarming language like, "Your account has now been put on hold," or "Unusual Activity Report," with a bogus "Solutions" link to restore the recipient's account. Unexpected tax refunds are another potential target for scam artists.

Never click on any unsolicited communication claiming to be the IRS, as it may surreptitiously load malware. Hackers may also be trying to load ransomware that keeps legitimate users from accessing their systems and files.

You should never respond to tax-related phishing or smishing or click on the URL link. The IRS initiates most contact through regular mail. If a taxpayer receives an unsolicited email claiming to be from the IRS, report it by sending it as an attachment to phishing@irs.gov. The report should include the caller ID (email or phone number), date, time, time zone, and the number that received the message.

Steer clear of abusive Employee Retention Credit claims

The IRS continues to warn businesses to stay clear of unscrupulous and aggressive promoters of questionable claims for Employee Retention Credits (ERCs). You may have noticed a sharp decrease in their ads toward the end of 2023. Third-party promoters of the ERCs often don't accurately explain eligibility for and computation of the credit. Additionally, some advertisements exist solely to collect the taxpayer's personal information in exchange for false promises. The IRS has taken steps to counter aggressive marketing around the ERCs, including a moratorium on processing new claims filed after September 14, 2023. The agency also has been reminding businesses that they can withdraw any unprocessed claims, which would avoid future repayment, interest, and penalties.

Don't accept IRS online account help from third-party scammers

Swindlers target individuals by posing as a helpful third party and offering to create a taxpayer's IRS online account at IRS.gov. Third parties making these offers will try to steal a taxpayer's personal information and sell it to others to use to file fraudulent tax returns, obtain loans, or open credit card accounts. You should remember you can set these accounts up yourself. You should not use third-party assistance other than the approved IRS authentication process through IRS.gov to create your IRS online account.

Don't make false fuel tax credit claims

The IRS continues to focus on improper credits. The fuel tax credit is for off-highway business and farming use. The credit is not available to most taxpayers. However, unscrupulous tax-return preparers and promoters are enticing taxpayers to inflate their refunds by erroneously claiming the credit. Promoters are focused on their own gain, taking advantage of the taxpayer with inflated fees, refund fraud, and identity theft.

Watch out for Offer in Compromise mills

The Offer in Compromise (OIC) program allows some taxpayers to work with the IRS to settle a tax debt for less than the full amount owed. These agreements are made directly between the taxpayer and the IRS, without a third party. However, so-called OIC mills often mislead taxpayers into believing they can settle a tax debt for pennies on the dollar. The scams are promoted to people who don't meet the qualifications for the OIC program, and taxpayers are frequently charged excessive fees. Taxpayers can make the same deal directly with the IRS without paying a fee. You can check your OIC eligibility for free by using the IRS's Offer in Compromise Pre-Qualifier tool.

IRS Releases Its Dirty Dozen Tax Scams and Schemes for 2024

Don't be fooled by fake charities

Beware of scammers using fake charities, especially following major disasters. Scammers often try to prey on well-intentioned donors by posing as fake charities, hoping to steal money and personal and financial data that can be used in tax-related identity theft. Taxpayers should never feel pressured to give immediately. Legitimate charities are happy to get a donation at any time. Take time to do your own research. You should never make donations using a gift card or by wiring money. It is safest to pay by credit card or check.

Be afraid of ghosts

Taxpayers should be wary of preparers who encourage people to file false tax returns, which could also be a ruse for stealing valuable personal information. One such type is a ghost preparer who encourages taxpayers to take advantage of tax credits and benefits for which they do not qualify. These preparers can charge a large percentage of the refund (or even steal the entire refund). After the return is done, these ghost preparers disappear. Warning signs include the preparer charging a fee based on the size of the refund, refusing to sign a tax return, or asking you to sign a blank or incomplete return. The IRS advises choosing a tax professional carefully. The agency offers a variety of resources to help, including a Directory of Federal Tax Return Preparers with Credentials and Select Qualifications. The directory is searchable and sortable.

Watch for misleading social media tax advice

Be careful of relying on what you read on social media, especially anything tax-related. Some internet advice contains fraudulent tactics promoted by scammers or false tax-related schemes that trend across popular social media platforms. The IRS is aware of various filing season hashtags and social media topics leading to inaccurate and potentially fraudulent information. The central theme involves people trying to use legitimate tax forms for the wrong reason. One recent scheme involves Form 8944 fraud (Preparer e-File Hardship Waiver Request), touted as a form the average taxpayer can use to receive a refund from the IRS. Another scheme is Form W-2 fraud (Wage and Tax Statement), which encourages people to use tax software to fill out a W-2 manually and include false income information. Taxpayers should verify information on IRS.gov or other official IRS accounts, where detailed form instructions can be found. Anyone knowingly filing fraudulent tax returns faces significant civil and tax penalties.

Spearfishing attacks are still ongoing

Spearfishing was on the IRS list last year, but this year's focus is on attacks on tax professionals and businesses. Cybercriminals impersonate real taxpayers seeking help. They use fake emails to get sensitive data or gain access to a tax professional's client information from their computer systems. These attacks usually peak around tax season, but they remain a year-round threat. Criminals accessing tax preparer credentials, or their client's tax-related information, can affect multiple victims. Of specific concern are scams where identity thieves pose as potential new clients using fake emails.

Key Wealth

Some schemes target high-income filers

This year the IRS warned wealthy individuals about three tax traps designed for them by dishonest promoters and tax preparers. These tools can be misused by promoters who misapply rules and leave the filers vulnerable:

- **Improper art donation deductions**
  Promoters encourage taxpayers to buy various types of art at a discounted price and wait a year to claim a tax deduction for an inflated fair market value that is substantially more than what the taxpayer paid for it.
- **Charitable remainder annuity trusts (CRAT)**
  In this scheme, taxpayers are directed to transfer property to a CRAT and improperly claim that the transfer results in an increase in basis. As a result, upon sale of the property, no gain is recognized. Instead, the payment received is treated as a return of investment, for which no tax is due. Next, the CRAT purchases a single premium annuity with the proceeds from the sale of the property.
- **Monetized installment sales**
  Promoters facilitate a purported monetized installment sale for the taxpayer in exchange for a fee. The installment note typically provides for payments of interest only, with principal being paid at the end of the term. This is structured to improperly delay the recognition of gain on the appreciated property until the final payment of the installment note.

Be suspicious of tax avoidance strategies

The IRS warns taxpayers about promoters selling bogus tax strategies designed to reduce or avoid taxes altogether, including:

- **Syndicated conservation easements**
  In abusive arrangements, promoters are syndicating conservation easement transactions that purport to give an investor the opportunity to claim charitable contribution deductions and corresponding tax savings that significantly exceed the amount invested. These abusive arrangements, which generate high fees for promoters, attempt to game the tax system with grossly inflated tax deductions.
- **Micro-captive insurance arrangements**
  Abusive micro-captives involve schemes that lack many of the attributes of legitimate insurance. These structures often include implausible risks, failure to match genuine business needs, and in many cases, unnecessary duplication of the taxpayer's commercial coverages. In addition, the premiums paid under these arrangements are often excessive, reflecting non-arm's-length pricing.

There are still more bogus schemes

Some of these include international elements:

- **Maltese individual retirement arrangement misusing treaty**
  U.S. taxpayers attempt to avoid tax by contributing to a foreign individual retirement arrangement in Malta (or potentially other host countries). These participants lack any local connection to the host country. They improperly assert that the foreign arrangement is a pension fund for US tax treaty purposes and exempt from US income taxation on gains, earnings, and distributions from the foreign individual retirement arrangement.
- **Digital assets**
  The IRS continues to scrutinize taxpayers attempting to hide assets in offshore accounts and accounts holding digital assets, such as cryptocurrency. Unscrupulous promoters lure US citizens into placing their assets in offshore accounts and structures, saying that they are out of reach of the IRS. Or promoters recommend digital assets as being untraceable and undiscoverable by the IRS. They promise tax savings that are too good to be true and will likely cause harm to taxpayers. The truth is that the IRS can identify and track anonymous transactions of digital assets around the globe.

The IRS places a high priority on abusive transactions and schemes and is always on the lookout for promoters and participants of these types of schemes. Where appropriate, the IRS will challenge them and impose penalties. As part of the Dirty Dozen awareness effort regarding tax schemes and unscrupulous tax preparers, the IRS urges individuals to report those who promote abusive tax practices or intentionally file incorrect returns.

How to protect yourself: Security reminders for taxpayers

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 protect you

Make sure your institution has implemented processes to protect your private, banking, and financial information. These include multi-factor authentication, call-back verification for certain transactions, and email encryption programs. 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 for 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

Don't give out Social Security numbers or passwords to anyone who solicits a charitable contribution.

Use IP PINs

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 settings 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.

For more information about preventing tax fraud, please contact your advisor.

Key Wealth

The Key Wealth Institute is a team of highly experienced professionals representing various disciplines within wealth management who are dedicated to delivering timely insights and practical advice. From strategies designed to better manage your wealth, to guidance to help you better understand the world impacting your wealth, Key Wealth Institute provides proactive insights needed to navigate your financial journey.

About the Author

As a Senior Wealth Planner for Key Private Bank, Paul focuses on ensuring his clients' wealth management plans are carried through to meet their unique financial objectives and grow and preserve wealth.

Paul most recently served as a Regional Planning Strategist for Key Private Bank. Prior to joining Key, Paul was the director of Wealth Planning at Wilmington Trust and was responsible for the delivery of planning services and the planning platform, including scalable advice-oriented solutions, thought leadership, and direct planning where appropriate. Paul contributed thought leadership and solutions to the Corporate Executive Practice Group, including direct planning for corporate executives. Prior to joining M&T Bank, which acquired Wilmington Trust in 2011, Paul was a tax manager with a CPA firm.

He holds an MBA from SUNY Buffalo and completed their Graduate Tax program. Paul is a Certified Public Accountant and a Chartered Global Management Accountant and has the Certified Financial Planner®, Personal Financial Specialist, Certified Life Underwriter, Retirement Income Certified Professional®, Certified Advisor in Philanthropy, Chartered Advisor in Senior Living, Chartered Financial Consultant, and Certified Retirement Counselor designations. Paul instructed courses in the Certified Financial Planner Program as an adjunct faculty member of Canisius College in Buffalo New York. He is currently the treasurer and member of the board of directors for Musicalfare Theater in Amherst, New York. Previously, he served on the board of directors and as the treasurer of the Make-A-Wish Foundation of Western New York and BNSME. Paul is a member of the FPA, AICPA, and NYSSCPA.

Key Wealth

240501-2580678