IRS

IRS wraps up 2023 Dirty Dozen list; reminds taxpayers and tax pros to be wary of scams and schemes, even after tax season

IR-2023-71, April 5, 2023

WASHINGTON — The Internal Revenue Service wrapped up the annual Dirty Dozen list of tax scams for 2023 with a reminder for taxpayers, businesses and tax professionals to watch out for these schemes throughout the year, not just during tax season.

Many of these schemes peak during filing season as people prepare their tax returns. In reality, these scams can occur throughout the year as fraudsters look for ways to steal money, personal information, data and more.

To help people watch out for these scams, the IRS and the Security Summit partners are providing an overview recapping this year's Dirty Dozen scams.

"Scammers are coming up with new ways all the time to try to steal information from taxpayers," said IRS Commissioner Danny Werfel. "People should be wary and avoid sharing sensitive personal data over the phone, email or social media to avoid getting caught up in these scams. And people should always remember to be wary if a tax deal sounds too good to be true."

Working together as the Security Summit, the IRS, state tax agencies and the nation's tax industry, including tax professionals, have taken numerous steps since 2015 to warn people about common scams and schemes during tax season and beyond that can increase the risk of identity theft. The Security Summit initiative is committed to protecting taxpayers, businesses and the tax system from scammers and identity thieves.

Some items on this year's list were new and some made a return visit. While the list is not a legal document or a formal listing of agency enforcement priorities, it is intended to alert taxpayers and the tax professional community about various scams and schemes.

2023 Dirty Dozen summary:

Employee Retention Credit claims

Taxpayers should be aware of aggressive pitches from scammers who promote large refunds related to the Employee Retention Credit (ERC). The warning follows blatant attempts by promoters to con ineligible people to claim the credit. The IRS highlighted these schemes from promoters who have been blasting ads on radio and the internet touting refunds involving Employee Retention Credits. These promotions can be based on inaccurate information related to eligibility for and computation of the credit. Additionally, some of these advertisements exist solely to collect the taxpayer's personally identifiable information in exchange for false promises. The scammers then use the information to conduct identity theft.

Phishing and smishing

Taxpayers and tax professionals should be alert to fake communications from those posing as legitimate organizations in the tax and financial community, including the IRS and the states. These messages arrive in the form of an unsolicited text (smishing) or email (phishing) to lure unsuspecting victims to provide valuable personal and financial information that can lead to identity theft. The IRS initiates most contacts through regular mail and will never initiate contact with taxpayers by email, text or social media regarding a bill or tax refund.

Online account help from third-party scammers

Swindlers pose as a "helpful" third party and offer to help create a taxpayer's IRS Online Account at IRS.gov. In reality, no help is needed. The online account provides taxpayers with valuable tax information. But third parties making these offers will try to steal a taxpayer's personal information this way. Taxpayers can and should establish their own online account through IRS.gov.

False Fuel Tax Credit claims

The fuel tax credit is meant for off-highway business and farming use and, as such, 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. The IRS has seen an increase in the promotion of filing certain refundable credits using Form 4136, Credit for Federal Tax Paid on Fuels.

Fake charities

Bogus charities are a perennial problem that gets bigger whenever a crisis or natural disaster strikes. Scammers set up these fake organizations to take advantage of the public's generosity. They seek money and personal information, which can be used to further exploit victims through identity theft.

Taxpayers who give money or goods to a charity might be able to claim a deduction on their federal tax return if they itemize deductions, but charitable donations only count if they go to a qualified tax-exempt organization recognized by the IRS.

Unscrupulous tax return preparers

Most tax preparers provide outstanding and professional service. However, people should be careful of shady tax professionals and watch for common warning signs, including charging a fee based on the size of the refund. A major red flag or bad sign is when the tax preparer is unwilling to sign the dotted line. Avoid these "ghost" preparers, who will prepare a tax return but refuse to sign or include their IRS Preparer Tax Identification Number (PTIN) as required by law. Taxpayers should never sign a blank or incomplete return.

Social media: Fraudulent form filing and bad advice

Social media can circulate inaccurate or misleading tax information, and the IRS has recently seen several examples. These can involve common tax documents like Form W-2 or more obscure ones like Form 8944. While Form 8944 is real, it is intended for a very limited, specialized group. Both schemes encourage people to submit false, inaccurate information in hopes of getting a refund. Taxpayers should always remember that if something sounds too good to be true, it probably is.

Spearphishing and cybersecurity for tax professionals

Phishing is a term given to emails or text messages designed to get users to provide personal information. Spearphishing is a tailored phishing attempt to a specific organization or business.

The IRS is warning tax professionals about spearphishing because there is greater potential for harm if the tax preparer has a data breach. A successful spearphishing attack can ultimately steal client data and the tax preparer's identity, allowing the thief to file fraudulent returns.

Offer in Compromise mills

Offers in Compromise are an important program to help people who can't pay to settle their federal tax debts. But "mills" can aggressively promote Offers in Compromise in misleading ways to people who clearly don't meet the qualifications, frequently costing taxpayers thousands of dollars. A taxpayer can check their eligibility for free using the IRS Offer in Compromise Pre-Qualifier tool.

Schemes aimed at high-income filers

- **Charitable Remainder Annuity Trust (CRAT):** Charitable Remainder Trusts are irrevocable trusts that let individuals donate assets to charity and draw annual income for life or a specific period. Unfortunately, these trusts are sometimes misused by promoters, advisors and taxpayers to try to eliminate ordinary income and/or capital gain on the sale of the property.
- **Monetized Installment Sales:** In these potentially abusive transactions, promoters find taxpayers seeking to defer the recognition of gain upon the sale of appreciated property. They facilitate a purported monetized installment sale for the taxpayer in exchange for a fee.

Bogus tax avoidance strategies

- **Micro-captive insurance arrangements:** A micro-captive is an insurance company whose owners elect to be taxed on the captive's investment income only. 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.
- **Syndicated conservation easements**: A conservation easement is a restriction on the use of real property. Generally, taxpayers may claim a charitable contribution deduction for the fair market value of a conservation easement transferred to a charity if the transfer meets the requirements of Internal Revenue Code 170. In abusive arrangements, which generate high fees for promoters, participants attempt to game the tax system with grossly inflated tax deductions.

Schemes with international elements

- **Offshore accounts and digital assets:** The IRS continues to scrutinize attempts to hide assets in offshore accounts and accounts holding digital assets, such as cryptocurrency. The IRS continues to identify individuals who attempt to conceal income in offshore banks, brokerage accounts, digital asset accounts and nominee entities. Asset protection professionals and unscrupulous promoters continue to lure U.S. persons into placing their assets in offshore accounts and structures saying they are out of reach of the IRS. These assertions are not true. The IRS can identify and track anonymous transactions of foreign financial accounts as well as digital assets.
- **Maltese individual retirement arrangements misusing treaty**: These arrangements involve U.S. citizens or residents who attempt to avoid U.S. tax by contributing to foreign individual retirement arrangements in Malta (or potentially other host countries). The participants in these transactions typically lack any local connection to the host country. By improperly asserting the foreign arrangement as a "pension fund" for U.S. tax treaty purposes, the U.S. taxpayer misconstrues the relevant treaty provisions and improperly claims an exemption from U.S. income tax on gains and earnings in and distributions from the foreign individual retirement arrangement.
- **Puerto Rican and foreign captive insurance**: U.S. business owners of closely held entities participate in a purported insurance arrangement with a Puerto Rican or other foreign corporation in which the U.S. business owner has a financial interest. The U.S. business owner (or a related entity) claims a deduction for amounts paid as premiums for "insurance coverage" provided by a fronting carrier, which reinsures the "coverage" with the Puerto Rican or other foreign corporation. Despite being labeled as insurance, these arrangements lack many of the attributes of legitimate insurance.

Where appropriate, the IRS will challenge the purported tax benefits from these types of transactions and impose penalties. The IRS Criminal Investigation Division is always on the lookout for promoters and participants of these types of schemes. Taxpayers should think twice before including questionable arrangements like this on their tax returns. After all, taxpayers are legally responsible for what's on their return, not a promoter making promises and charging high fees. Taxpayers can help stop these arrangements by relying on reputable tax professionals they know and trust.

Help stop fraud and scams

As part of the Dirty Dozen awareness effort, the IRS encourages people to report individuals who promote improper and abusive tax schemes as well as tax return preparers who deliberately prepare improper returns.

To report an abusive tax scheme or a tax return preparer, people should mail or fax a completed Form 14242, Report Suspected Abusive Tax Promotions or Preparers PDF and any supporting material to the IRS Lead Development Center in the Office of Promoter Investigations.

Mail:

Internal Revenue Service Lead Development Center
Stop MS5040
24000 Avila Road
Laguna Niguel, California 92677-3405
Fax: 877-477-9135

Alternatively, taxpayers and tax practitioners may send the information to the IRS Whistleblower Office for

possible monetary reward. For more information, see Abusive Tax Schemes and Abusive Tax Return Preparers.

Page Last Reviewed or Updated: 05-Apr-2023