Hawthorne & Co.
Certified Public Accountants

IRS ANNOUNCES "DIRTY DOZEN" TAX SCAMS FOR 2021

From the Internal Revenue Service – News Release: IR-2021-135

The Internal Revenue Service, on Monday, June 28, began its "Dirty Dozen" list for 2021 with a warning for taxpayers, tax professionals and financial institutions to be on the lookout for these 12 nefarious schemes and scams.

This year's "Dirty Dozen" will be separated into four separate categories:

- **pandemic-related scams** like Economic Impact Payment theft
- **personal information cons** including phishing, ransomware and phone "vishing"
- **ruses focusing on unsuspecting victims** like fake charities and senior/immigrant fraud
- **schemes that persuade taxpayers into unscrupulous actions** such as Offer In Compromise mills and syndicated conservation easements.

The agency compiled the list into these categories based on who perpetuates the schemes and who they impact.

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.

"We continue to see scam artists use the pandemic to steal money and information from honest taxpayers in a time of crisis," said IRS Commissioner Chuck Rettig. "We provide this list to alert taxpayers about common scams that fraudsters use against their victims. At the IRS, we are dedicated to stopping these criminals, but it's up to all of us to remain vigilant to protect ourselves and our families."

Taxpayers are encouraged to review the "Dirty Dozen" list in a special section on IRS.gov and should be alert to these scams during tax filing season and throughout the year.

Economic Impact Payment theft

A continuing threat to individuals is from identity thieves who try to steal Economic Impact Payments (EIPs), also known as stimulus payments. Most eligible people will get their payments automatically from the IRS. Taxpayers should watch out for these tell-tale signs of a scam:

- Any text messages, random incoming phone calls or emails inquiring about bank account information or requesting recipients to click a link or verify data should be considered suspicious and deleted without opening.
- Be alert to mailbox theft. Frequently check mail and report suspected mail losses to Postal Inspectors.
- Don't fall 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.

Taxpayers should remember that 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

Because of the COVID-19 pandemic, many taxpayers lost their jobs and received unemployment compensation from their state. However, scammers also took advantage of the pandemic by filing 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.

The IRS reminds taxpayers to be on the lookout for receiving a Form 1099-G reporting unemployment compensation that they didn't receive. For people in this situation, the IRS urges them to contact their appropriate state agency for a corrected form. If a corrected form cannot be obtained so that a taxpayer can file a timely tax return, taxpayers should complete their return claiming only the unemployment compensation and other income they actually received. See Identity Theft and Unemployment Benefits for tax details and DOL.gov/fraud for state-by-state reporting information.

Additional protection to help protect taxpayers

IRS makes IP PINs available to all taxpayers – adding another layer of security

To help taxpayers avoid identity theft, the IRS this year made its Identity Protection PIN (IP PIN) program available to all taxpayers. 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.

Reducing fraud

The IRS and its Security Summit partners in the states and the private-sector tax community have made changes to help reduce identity theft-related refund fraud that are noticeable to the average person filing a return:

- Tax software providers agreed to strengthen password protocols. This is the first line of defense for these companies to make sure their products are secure.
- State tax agencies began asking for taxpayers' driver's license numbers as another way for people to prove their identities.
- The IRS limited the number of tax refunds going to financial accounts or addresses.
- The IRS masked personal information from tax transcripts.

Hawthorne & Co.
Certified Public Accountants

Multi-factor authentication can help

It is important for taxpayers filing in 2021 to know that online tax software products available to both taxpayers and tax professionals will contain options for multi-factor authentication. 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.

The IRS and its Security Summit partners have formed an information sharing center that allows them to quickly identify emerging scams and react to protect taxpayers. The Identity Theft Tax Refund Fraud Information Sharing and Analysis Center is now operational.

Also, check out our recent A Closer Look column for more on how to be vigilant about tax scams. Visit Identity Theft Central and Tax Fraud Alerts for more information on how to protect against or report identity theft or fraud.