The IRS Announces Tax Scams

Compiled annually, the IRS lists a variety of common scams that taxpayers can encounter. This year's list includes the following four categories.

- **Pandemic-related scams.** Criminals are still using the COVID-19 pandemic to steal people's money and identity with phishing emails, social media posts, phone calls, and text messages. Scammers steal personal information and use it to file fraudulent tax returns. Be on the look out for Economic Impact Payment and tax refund scams, unemployment fraud leading to inaccurate taxpayer 1099-Gs, fake employment offers on social media and fake charities that steal taxpayers' money.
- **Offer-in-compromise mills** (OIC). This type of scam makes outlandish claims about how they can settle a person's tax debt for pennies on the dollar. Often, the reality is that taxpayers are required to pay a large fee upfront to get the same deal they could have gotten on their own by working directly with the IRS. These services tend to be more visible right after the filing season ends while taxpayers are trying to pay their recent bill.
- **Suspicious communication**. Criminals use a variety of communications designed to trick, surprise, or scare someone into responding before thinking. The IRS warns taxpayers to be on the lookout for suspicious activity across four common forms of communication: email, social media, telephone, and text messages. Victims are tricked into providing sensitive personal financial information, money, or other information. This information can be used to file false tax returns and tap into financial accounts, among other schemes.
- **Spear phishing attacks**. Criminals try to steal client data and tax preparers' identities to file fraudulent tax returns for refunds. Spear phishing can be tailored to attack any type of business or organization, so everyone needs to be skeptical of emails requesting financial or personal information.

What you can do. If you discover that you're a victim of identity theft, consider taking the following action:

1. **Notify creditors and banks**. Most credit card companies offer protections to cardholders affected by ID theft. Generally, you can avoid liability for unauthorized charges exceeding $50. But if your ATM or debit card is stolen, report the theft immediately to avoid dire consequences.
2. **Place a fraud alert on your credit report**. To avoid long-lasting impact, contact any one of the three major credit reporting agencies-Equifax, Experian or TransUnion-to request a fraud alert. This covers all three of your credit files.
3. **Report the theft to the Federal Trade Commission (FTC)**. Visit identitytheft.gov or call 877-438-4338. The FTC will provide a recovery plan and offer updates if you set up an account on the website.

Source: Barry J. Pierce, CPA, The Kaufman Herald, Aug 4, 2022