Heinold Banwart, Ltd.
Certified Public Accountants

Third Floor
201 Clock Tower Drive
East Peoria, IL 61611-2449

Tel (309) 694-4251
Fax (309) 694-4202
Web www.hbcpas.com

IRS Cracks Down on Tax ID Theft: Could You Be a Victim?

For the past several years, the IRS has been cracking down on a frightening problem: identity theft schemes that are aimed at stealing taxpayers' refunds. When this type of fraud occurs, an individual's refund can be delayed for months or longer. Here's a look at how tax identity theft works, along with steps you can take to help protect yourself from becoming a victim — and what to do if your identity is stolen.

A Typical Tax ID Crime

An identity thief generally uses a legitimate taxpayer's identity and Social Security number to fraudulently file a tax return and claim a refund. This is usually done early in the tax filing season. The victim typically finds out about the fraud after he or she files a tax return and is informed by the IRS that the return has been rejected because the Social Security number has already been used to file a tax return for the same tax year. The IRS then delays processing the refund until it can determine who the legitimate taxpayer is.

How do thieves obtain Social Security numbers? They may hack into victims' computers or the unsecured websites and networks of businesses, or they might steal wallets or purses, rummage through trash or steal statements from mailboxes. Sometimes, criminals make phone calls claiming to be from businesses that need information. Other times, they buy information from informants who have access to Social Security numbers at their jobs.

The IRS itself was hacked earlier this year, and thieves stole information from approximately 100,000 accounts. The data breach affected taxpayers who used the "Get Transcript" application on the IRS website.

If you're an employer, you can also be a victim of tax identity theft. The Employer Identification Number of a real organization could be fraudulently used to report fake earnings and withholding. The IRS may issue a refund to the thief before it realizes that there is no matching, legitimate paperwork from an employer.

How To Protect Yourself

There's no way to fully shield yourself from tax-related identity theft but there are steps you can take to minimize the chances — or at least to identify a possible theft early to reduce the damage:

- Don't give out your Social Security number to businesses or medical providers just because they ask for it. Provide it only when required. The Social Security Administration advises consumers to "ask why your number is needed, how it will be used and what will happen if you refuse."
- Protect your financial information. Shred documents with personal identifying information. Don't provide information in response to email or text messages. Don't give personal information over the phone unless you initiated the contact or you know whom you're dealing with. Don't carry your Social Security card or documents with your number on them. Keep these in a safe place at home.

- Don't respond to phishing schemes. The IRS doesn't get in touch with taxpayers by email or text message to request personal information. An initial contact from the IRS about your tax return comes in the form of correspondence through the U.S. mail.
- Protect personal computers by using firewalls, anti-spam/virus software and updated security patches.
- Regularly change passwords for online accounts.
- Check your credit report at least every 12 months for any suspicious activity.
- Review your Social Security Administration earnings statement annually to ensure there are no reporting problems with your records. Set up an account at *www.socialsecurity.gov/myaccount*.
- And, of course, file your income tax return as early as possible in the tax filing season.

Tax Identity Theft May Not End at Death

Each year, according to the IRS, thieves steal the identities of nearly 2.5 million deceased Americans. Refunds can be stolen from the estates of individuals. If you are an executor or personal representative of an estate, send the IRS a copy of the death certificate. The tax agency will use it to flag the account that the person is deceased.

If You Become a Victim

Respond immediately if you receive an IRS letter or notice stating that another return has been filed with your information or that you received wages from an employer other than your actual one. You may be asked to confirm your identification on the IRS website through the Identity Verification Service (IDVerify) or by phone at the IRS toll-free number provided in the letter. You should also prepare and submit an Identity Theft Affidavit on IRS Form 14039.

If you're a victim of tax identity theft, you should also get an Identification Number from the IRS that proves you are the legitimate filer of future tax returns. The IRS issues an Identity Protection Personal Identification Number (IP PIN) to identity theft victims whose identities have been validated. It allows legitimate returns to be processed and prevents processing of fraudulent returns. That can mitigate processing delays in victims' federal tax return processing.

Generally, the IP PIN is mailed out once the taxpayer's account has been resolved. Current programming allows one IP PIN to be generated each year.

In addition to contacting the IRS, the government recommends that an identity theft victim file a complaint with the FTC at http://www.consumer.ftc.gov and file a local police report. You should close any accounts opened without your permission and notify one of the major credit bureaus (Equifax, Experian or TransUnion) to place a fraud alert on your credit file.

Take Identity Theft Seriously

Tax return fraud can cause major headaches to straighten out and significantly delay legitimate refunds. Let us know if you have concerns about fraud and your tax return. We can help.

Sincerely,

HEINOLD BANWART, LTD.