Scammers Impersonating IRS Agents Called You Yet?

Article Highlights:

- Scams Impersonating IRS Agents
- Protecting Against Scams
- Protecting Against ID Theft
- What to Do If Your ID Has Been Compromised

The Treasury Inspector General for Tax Administration (TIGTA) has indicated it is making significant progress in its investigation of the IRS impersonation scams that are sweeping the nation, causing reported taxpayer losses of more than $36 million and averaging more than $5,700 per taxpayer. To date, TIGTA has logged approximately 1.2 million calls reported by taxpayers, and nearly 6,400 people have reported that IRS impersonators have fleeced them.

In one instance, a taxpayer was so convinced the scammer was an IRS agent he rushed off to make a payment and was involved in a traffic accident. He was so worried about the scammer's threats of legal action that he actually left the scene of the accident so he could promptly get the funds wired to the scammer. In this case TIGTA was able to trace the victim's wire transfer and ultimately nabbed a ring of five scammers.

But these stories generally don't have happy endings, so it is important for everyone to understand that the IRS never demands payment by wire, MoneyGram, debit cards or the like, and it always makes initial contact by mail.

Protect Yourself and Loved Ones from Being a Scam Victim:

1. Hang up on callers claiming to be IRS agents, IRS collection agents or state taxing authorities demanding immediate payments. They are not legitimate.
2. Take the time to educate your loved ones, especially those who might be vulnerable, about these scams and take steps necessary to protect them from scams.
3. Call this office if you need assurances or wish to confirm you do not have an outstanding balance with a tax authority.
4. Report scams and attempted scams on the TIGTA website.

Protect Against Identity Theft – In addition to scammers, watch out for those ID thieves out there looking for vulnerable IDs to steal. You may think it will never happen to you, but if it does, it will become a nightmare and could take years to straighten out. So you need to protect yourself against ID theft by limiting the exposure of your personal and financial information as much as possible.

What do ID thieves need to create havoc for you? Your name, Social Security number and birth date! Here are some tips to limit your ID exposure:

- Don't carry your Social Security card – or any document that includes your Social Security number (SSN), for that matter – in your wallet, purse or briefcase. Your Social Security card combined with your driver's license provides scammers with the three pieces of information they need.
- Don't give out either your SSN or your birth date without questioning the need and making sure it is a legitimate request and really necessary.
- Limit the number of credit cards and credit accounts you have. Each account has your SSN, so the more accounts you have, the greater the chance you'll

be caught up in a data breach and your ID will be compromised. It is far easier to deal with one credit card company than several if your ID is breached.

- Be proactive and periodically change the passwords for your online accounts that include sensitive financial information. It is a pain, but it could avoid you a major headache.
- Although only the last four digits of your SSN are used on most financial documents, you should still pay close attention to documents that include your full SSN or birth date. Limit their duplication and distribution and ensure they are properly disposed of when you discard them.
- Never include your SSN, birthdate or other sensitive financial information in an e-mail or in documents attached to an e-mail.

Use common sense and follow the "need-to-know" rule when disclosing your financial information. Careless safeguarding of your information can lead to big problems.

Think Your ID Has Been Compromised? You should immediately:

- File a complaint with the Federal Trade Commission at www.identitytheft.gov and complete a report. In addition to taking the report, the site will develop an ID Theft Affidavit that you can use when reporting the ID theft to creditors and others. The site will also walk you through various steps to be taken depending upon the specifics of your ID theft.
- Contact one of the three major credit bureaus to place a "fraud alert" on your credit records and review your credit report for fraudulent activity:
    - Equifax, www.Equifax.com, 1-800-766-0008
    - Experian, www.Experian.com, 1-888-397-3742
    - TransUnion, www.TransUnion.com, 1-800-680-7289
- Contact your financial institutions and close any financial or credit accounts opened without your permission or tampered with by identity thieves.
- Report any fraud to your local police and retain a copy of the police report to use when reporting fraud to other agencies or creditors.

You should also contact this office immediately so steps can be taken to avoid fraudulent returns being filed using your SSN. Even if someone has already e-filed a return and claimed a refund under your SSN, your refund may still be safe.

However, you cannot e-file and instead must file a paper return with the proper documentation; you will ultimately receive the refund you are due, but it will be severely delayed. Once the IRS recognizes that your SSN was used to file a fraudulent return, it will block your SSN from filing and assign you an alternative filing number for the subsequent year.

For more information on how and what to file when someone else has filed using your SSN, please contact this office.