IRS FACT SHEETS DESCRIBE WAYS TO COMBAT TAXPAYER IDENTITY THEFT

Fact Sheet 2015-1, January 2015, Fact Sheet 2015-2, February 2015

In two Fact Sheets, IRS has listed numerous ways that taxpayers can protect themselves from identity theft and the steps they should take if they find they have become victims of such fraud.

Background. IRS continues to increase its efforts against refund fraud, which includes identity theft. As a result of these aggressive efforts to combat identity theft from 2011 through October 2014, IRS has stopped 19 million suspicious returns and protected more than $63 billion in fraudulent refunds.

For 2015, IRS will continue to increase both the number and efficiency of the identity theft data models and filters that are used to identify potentially fraudulent returns. These pre-refund filters stop the vast majority of fraudulent returns. IRS also continues to expand its partnerships with financial institutions to identity and stop fraudulent refunds.

Starting January 2015, IRS also will limit the number of direct deposit refunds to a single financial account or pre-paid debit card to three. Fourth and subsequent valid refunds will convert to paper checks and be mailed to the taxpayer. The limit also will stop certain tax preparers who improperly deposit client refunds into their own accounts.

Fighting identity theft is an ongoing battle as identity thieves continue to create new ways of stealing personal information and using it for their gain. Tax-related identity theft occurs when someone uses a stolen Social Security (SS) number to file a tax return to claim a fraudulent refund. A taxpayer's SSN can be stolen through a data breach, a computer hack or a lost wallet. Although identity theft affects a small percentage of tax returns, it can have a major impact on victims by delaying their refunds.

Protecting oneself. IRS listed a number of simple, practical steps that a taxpayer can take to avoid becoming a victim. It advised a taxpayer:

- Don't carry your Social Security card or any documents that include your SSN or Individual Taxpayer Identification Number (ITIN);
- Don't give a business your SSN or ITIN just because they ask. Give it only when required;
- Protect your financial information;
- Check your credit report every 12 months;
- Review your Social Security Administration earnings statement annually;
- Secure personal information in your home;
- Protect your personal computers by using firewalls and anti-spam/virus software, updating security patches and changing passwords for Internet accounts; and

- Don't give personal information over the phone, through the mail or on the Internet unless you have initiated the contact or you are sure you know who you are dealing with.

Warning Signs. IRS provided possible indications that there has been a tax-related identity theft. It advised that a taxpayers should be on guard if he or she receive a notice from IRS or learn from their tax professional that:

- More than one tax return was filed for you;
- You owe additional tax, have a refund offset or have had collection actions taken against you for a year you did not file a tax return;
- IRS records indicate you received more wages than you actually earned; or
- Your state or federal benefits were reduced or cancelled because the agency received information reporting an income change.

Steps to take. IRS advised that all victims of tax-related identity theft should:

- File a report with the local police;
- File a complaint with the Federal Trade Commission (FTC) or the FTC Identity Theft hotline:
- Contact one of the three major credit bureaus to place a "fraud alert' on your account (Equifax, Experian, or TransUnion); and
- Close any accounts that have been tampered with or opened fraudulently.

In addition, if a taxpayer's SSN has been compromised and the taxpayer knows or suspects he or she may be a victim of tax-related identity theft, a taxpayer should:

- Respond immediately to any IRS notice and call the number provided;
- Complete IRS Form 14039, Identity Theft Affidavit. Use a fillable form at IRS's website, print, then mail or fax according to instructions;
- Continue to pay your taxes and file your tax return, even if you must do so by paper; and
- If you previously contacted IRS and did not have a resolution, contact the Identity Protection Specialized Unit.

Steps IRS has taken. IRS notes that identity theft cases are among the most complex handled by IRS. It is continually reviewing processes and policies to minimize the incidence of identity theft and to help those who find themselves victimized. Among the steps underway to help victims:

- The IRS Identity Protection PIN (IP PIN) is a unique six digit number that is assigned annually to victims of identity theft for use when filing their federal tax return that shows that a particular taxpayer is the rightful filer of the return.

- IRS is offering certain taxpayers the opportunity to opt into the IP PIN program. These are taxpayers who may be unaware that they are identity theft victims but IRS identified them because their accounts have indications of identity theft.
- IRS will continue its IP PIN pilot program that allows taxpayers who filed tax returns last year from Florida, Georgia or the District of Columbia to opt into the IP PIN program.
- This year, IRS uses an online process through its website that will allow taxpayers who have an IP PIN requirement and lose their IP PIN to create an account and receive an IP PIN online.
- Victim case resolutions are extremely complex cases to resolve, frequently touching on multiple issues and multiple tax years. A typical case can take 120 days to resolve, and IRS is working to streamline its internal process and reduce that time period.