How You Can Help Clients Dealing with Identity Theft

By Raymond J. Ziegler Jr., CPA

One of the worst feelings for a tax preparer is receiving an Internal Revenue Service rejection notice stating "The SSN you entered was used on someone else's tax return." The investigative work done by the IRS' Criminal Investigation Division is a major component of the agency's efforts to combat tax-related identity theft. In fiscal year 2012, the IRS initiated approximately 900 identity theft related criminal investigations, tripling the number initiated in fiscal year 2011. Since the start of this calendar year, the IRS has worked with victims to resolve and close more than 200,000 identity theft cases.

Usually, an identity thief uses a legitimate taxpayer's identity to fraudulently file a tax return and claim a refund. Generally, the identity thief will use a stolen SSN to file a forged tax return and attempt to get a fraudulent refund early in the filing season.

A tax preparer, in addition to the above rejection notice, can be alerted to possible identity theft if an IRS notice or letter that a taxpayer receives, states:

1. There is a balance due, refund offset or collection action has been taken against the taxpayer for a year a tax return was not filed, or
2. IRS records indicate the taxpayer received wages from an employer unknown to the taxpayer.

The tax preparer needs to respond immediately to a notice from the IRS if a taxpayer's tax records are affected by identity theft. Form 14039, Identity Theft Affidavit, will need to be completed. Also, the IRS suggests that you immediately file a paper return if the notice is a result of the taxpayer's SSN already being used on someone else's tax return. Victims of identity theft who have previously been in contact with the IRS and have not achieved a resolution can call the IRS Identity Protection Specialized Unit at (800) 908-4490.

As a result of filing Form 14039, the IRS will send a notice to the taxpayers indicating that an identity theft indicator has been placed on their account to protect them when filing their federal tax return. The IRS will review any tax return filed with their Taxpayer Identification Number to make sure it isn't being filed fraudulently. The notice provides a unique Identity Protection Personal Identification Number (IP PIN) to use when filing their tax return for the year indicated. The IP PIN is only good for one year, and a new one will be issued as long as the Identity Theft Indicator is on the taxpayer's account. The IRS has issued more than 770,000 IP PINs to identity theft victims at the start of the 2013 tax filing season.

Effective March 29, 2013, the IRS expanded, nationwide, a pilot program to help investigate identity theft. The Identity Protection PIN program allows taxpayer victims of identity theft to allow state and local law enforcement authorities to see the tax forms fraudulently filed in their name. Law enforcement representatives can then submit a disclosure authorization form, created by the IRS, to the Criminal Investigation Division, along with a copy of the police report and Form 14039, if available. The identity theft victim still needs to submit the original Form 14039 to the IRS.

A taxpayer's social security records may be affected as well. If wages were received from an unknown employer, the Social Security Administration also needs to be contacted.

How can taxpayers protect their tax records? If a taxpayer currently does not have tax records affected by identity theft but believes he or she may be at risk due to a lost/stolen purse or record, questionable credit card activity or credit report, he or she can call (800) 908-4490.

There are a number of ways for taxpayers to minimize the chance of being a victim:

1. Do not carry their Social Security card or any other document with their SSN on it.
2. Do not provide a business card with their SSN just because they are asked. Give it only when required.
3. Protect their financial information.
4. Check their credit report every 12 months.
5. Secure personal information in their home.
6. Protect their personal computers by using firewalls and anti-spam/virus software, updating security patches, and changing passwords for Internet accounts.
7. Do not give personal information over the phone, through the mail or on the Internet unless they have initiated the contact, or they are sure they know with whom they are dealing.

Raymond J. Ziegler Jr., CPA, is a senior manager in the tax department at Anders in St. Louis. Ray can be reached at rzieglerjr@anderscpa.com.