

http://www

Tax Times &

Potpourri

October 2016
Volume 1 Issue 76

Warren R Goldman CPA LLC, 10809 Childs Street, Silver Spring MD 20901
wrgoldman2@gmail.com 301 996 1050 240 206 3251 (fax)

Tax Related Identity Theft

INSIDE THIS ISSUE

- 1 Social Security Benefits
- 2 Tax Related Identity Theft
- 3 Tax Related Identity Theft
- 4 Editors Corner

Tax return identity theft occurs when a taxpayer's personal information such as name, social security number (SSN), employer identification number or other identifying information is used without the taxpayer's authority to file a fraudulent tax return (usually to claim a fraudulent refund or to obtain tax benefits). This type of identity theft carries serious consequences. It can take victims months just to prove their identity to the IRS, which in turn delays the processing of legitimate refund claims. Per the IRS, individual victims of identity theft may lose job opportunities, be refused loans, education housing or transportation, and may even be arrested for crimes they did not commit. For employers, they may incur significant damage to their reputations, financial losses and costs incurred to resolve issues with numerous agencies.

When an individual SSN has been compromised, the taxpayer may experience the following:

Continued on page 2

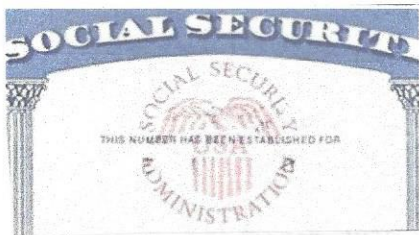
Social Security Benefits

Social security benefits can begin for an eligible worker at age 62. The current full retirement age at which benefits are not reduced is 66. If benefits are delayed past full retirement age, additional credits can be earned to age 70. Spouses, divorced spouses and widow(er)s may be eligible to collect on a worker's benefits at an earlier age. Regardless of the age at which benefits commence, the same tax rules apply.

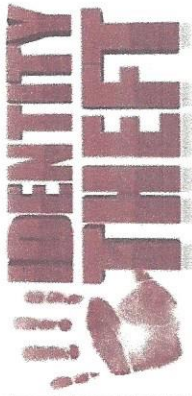
For federal income taxes, social security benefits may be tax-free or includible in gross income at 50% or 85%. High income taxpayers can assume that they are subject to the 85% inclusion amount. Others may have to do calculations too determine whether benefits are tax-free or the applicable percentage.

For state income tax purposes, the rules may be different. Twenty eight states and the District of Columbia fully exempt social security benefits from their income taxes. Other states have different income thresholds for taxing benefits than the income thresholds for federal income tax purposes.

If income is no more than a base amount, benefits are tax-free.



Income includes wages, interest, ordinary dividends, capital gain distributions and pensions, tax-exempt interest and 50% of social security benefits. The base amount is \$25000 if single, head of household, qualifying widower or married filing separately. The amount is \$32000 if married filing jointly.



Tax Related Identity Theft (continued from page 1)

The tax return is rejected usually with an IRS reject code that indicates the taxpayer SSN already has been used

The taxpayer receives a notice from the IRS requesting additional information to process the return accurately or an adjusted refund notice with changes to the Form 1040 when the taxpayer has not actually filed the return.

Business identity theft may be more difficult to detect than individual identity theft as the signs that indicate business identity theft may also be the product of a simple processing or filing error. The following are signs that warrant additional investigation:

The business files an original tax return but it is accepted as an amended tax return.

The IRS issues a notice to the business regarding fictitious employees or

The business discovers activity related to a business that is inactive or that has already been closed after all account balances pertaining to that entity have already been paid.

The taxpayer will need to contact the IRS to put a 'red flag' on the account due to identity theft. The identity theft indicator flags the taxpayer's identification numbers, along with any tax returns submitted in the future using the taxpayer's identification numbers so that the IRS can monitor the account for potential fraud. In addition, once the IRS puts an identity theft indicator on the taxpayer's account, it will not release any transcripts related to the account without further authentication.

The taxpayer will want to complete Form 14039 Identity Theft Affidavit but only for the specific individual who had his or her identity stolen. This form does not need to be completed for both the taxpayer and spouse if only one is a victim. If the fraud was discovered at the time of the notice or e-file (trying to file tax return electronically), the taxpayer needs to send Form 14039 in with the paper copy of the return. At this point, the tax return cannot be filed electronically. If the fraud was discovered when extending the return electronically, then Form 14039 will be faxed or mailed to the IRS as soon as possible.

The IRS may provide a fraud victim with an identity protection personal identification number (IP PIN) which is a six-digit number the taxpayer may use to verify the return's legitimacy. An IP PIN prevents someone else from filing a fraudulent return under the taxpayer's SSN. The IRS issues a new IP PIN every subsequent year.

Taxpayers should file a report with their local police department, report the identity theft to the Federal Trade Commission (FTC), contact one or more major credit bureaus to place fraud alert on their records, close any accounts opened fraudulently, and make their banks, lenders and credit card providers aware of the situation.

The actions for businesses that are victims of identity theft are similar to those recommended for individuals. In addition to notifications, above, a business should monitor their credit reports, online business information, and business account with the IRS and other state agencies (even for closed businesses). In addition, the business should review and update their computer security policies.

It usually takes the IRS 180 days to process an identity theft case after the taxpayer files Form 14039. At this point, the taxpayer cannot do much more until the IRS reviews the account and confirms the return's authenticity. It is common to experience delays in receiving refund due to the review of their account.

There are a number of recommendations that can be taken to prevent identity theft. Some suggestions may seem obvious but are very important. Taxpayers should shred important documents such as old tax returns, credit card and bank statements, medical bills and other records containing financial data. A taxpayer also needs to be cautious of emails from the IRS. The IRS does not send taxpayers email asking for personal and financial information.

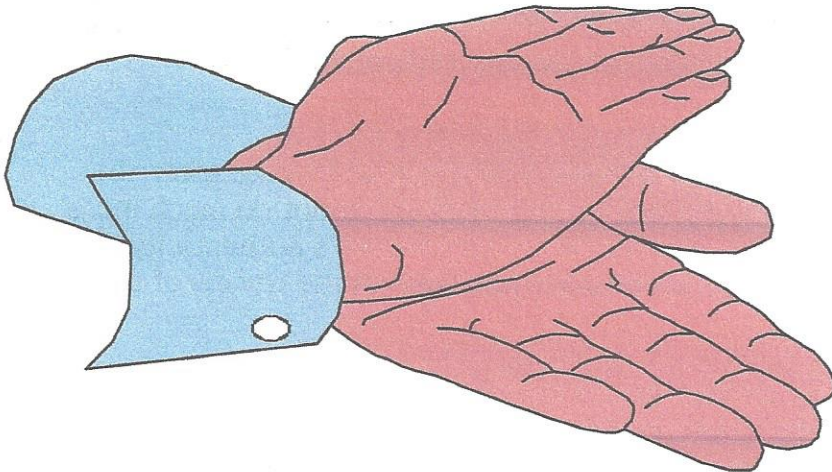
Additional advice includes:

1. Truncate SSNs where possible or mask SSNs on insurance cards.
2. Monitor credit reports at least annually.
3. Keep social security cards and financial information in a secure location and properly dispose of documents with SSNs or account numbers.
4. Give out an SSN, birthdate or address only if required.
5. Buy and use a shredder.
6. Protect personal computers with firewalls, anti-spam or anti-virus software, regularly change passwords and password secure wireless connections.
7. Be mindful of the personal information divulged on social media as hackers continue to get more sophisticated.

Business entities can follow the steps above. In addition, the business can add the following steps:

1. Use anti-virus and other security software on all office computers and update data security policies.
2. Educate employees about phishing (attempts by fraudsters to acquire information via electronic communications by posing as a legitimate entity).
3. Remind employees not to open links or attachments from emails they were not expecting to receive.
4. Update business filings with the IRS and with the secretary of state as soon as any contact information changes.
5. Monitor business credit profile.
6. If possible, consider filing business tax returns earlier in tax season.

7. Forward phishing emails purported to be from IRS per forwarding instructions on IRS website.



The 2016 Elections

I thought we had seen it all especially in the last presidential election in 2012 with name calling, under handed advertisements, questionable strategies, extreme media and social media coverage and lots of comedy.

Although the 2016 elections are now 39 days away, it definitely appears that 2012 will pale in comparison to what we have seen to date and what we will probably see over the next five plus weeks.

The news and analysis has come to a point where it almost is not necessary to watch the evening news, read the newspaper or follow the campaign stop speeches and events. All that one probably has to do is to open your Facebook page and watch the friends' posts. You probably have some Democratic friends and some Republican friends and you can rest assured that they will do all of the analysis for you and provide support for each political position.

Here is to surviving the election and I hope the candidates you support win on November 8th.

Warren R Goldman CPA LLC

10809 Childs Street
Silver Spring MD 20901

Phone:
301 996 1050

Fax:
240 206 3251

E-mail:
wrgoldman2@gmail.com

Website:
www.warrengoldmancpa.com