POINT TO REMEMBER

Identity Theft

By Robb A. Longman*

Identity theft is a growing problem nationwide. Individuals' identities are being stolen and used by others. The results to the victims are devastating. Identity thieves use a stolen personal identity to open credit card accounts, utility accounts, and other accounts and can easily ruin their victims' credit history. Identity thieves do not stop there. They may also use their victims' tax-related information, causing them problems with their tax return filings.

Taxpayers need to be aware of three types of identity theft. First, an identity thief may steal the taxpayer's identity and use the victim's social security number on a false tax return. That return will claim a refund. Second, an illegal worker may use the taxpayer's social security number. That results in additional income being reported to the Service. Third, a business may use an individual's social security number and report paying wages to that person even though the person did not work there. The business does this to reduce its taxable income and tax liability. Not only do these three actions cause havoc for both taxpayers and the Service, they cost the government significant lost revenue.

Discovering and Reacting to the Theft

When a taxpayer's identity is stolen and used to file a fraudulent tax return, the taxpayer usually does not find out immediately. It is usually difficult for the taxpayer to even find out at all. When a fraudulent tax return is filed, the thief uses an address other than that of the taxpayer. The Service then updates the taxpayer's account with the new address. All notices sent by the Service then go to the new address, which is usually a false address, and the victim does not receive any of them. The taxpayer typically finds out about this type of fraud after she files her tax return and it is rejected or an expected refund never arrives. Once that occurs, the taxpayer will have to provide documentation to demonstrate to the Service that she is in fact the owner of the social security number stolen. The items that constitute documentation are a copy of a driver's license or passport, a copy of the social security card, and a police report or FTC Affidavit of Identity Theft. By providing that information to the Service, the taxpayer has officially proven that she is who she says she is. The taxpayer's account should then be coded, and this should (hopefully) protect her account in the future.

With identity theft problems growing, the Service finally established a unit to specifically handle these issues. The new unit is the IRS Protection Specialized Unit and is reached at the Identity Theft Hotline at 1-800-908-4490.

It is unfortunately frequent that the taxpayer does not receive any notice of the fraud because the Service does not recognize that the abuse has occurred. In some circumstances, a taxpayer may not learn of the fraud until it is too late and collection activity has occurred on the account. When this occurs, it is imperative to respond immediately to the Service in order to protect the funds in jeopardy of being seized.

In some circumstances the Service will notice first that a taxpayer's social security number has been compromised. In those circumstances, it will request the same documentation listed above. If the taxpayer does not provide the information in a timely manner, his social security number will be frozen and he will be issued a taxpayer identification number until the matter is resolved.

When a taxpayer's social security number has been stolen and used for work purposes, the taxpayer will eventually receive a notice that he needs to file a tax return or that his tax return has been changed. The taxpayer must respond accordingly. In these situations, he must prove that he did not have income when it has been reported that income does exist. Usually he can demonstrate this by obtaining information from the employer reporting the wages or by showing that he did not live in or near the location from which the incorrect income was reported.

It is imperative that the taxpayer comply with the Service's requests in this situation to ensure that an assessment is not entered against him and that

*Joseph Greenwald & Laake PA, Greenbelt, MD.

collection activity does not occur. If collection activity has occurred, the taxpayer should follow regular avenues for disputing the tax assessed. The taxpayer can use the Offer in Compromise Program, ask for Audit Reconsideration, or go through the necessary channels to have the case heard in the United States Tax Court. In this situation, the burden of proving the taxpayer actually received the income will shift to the Service.

Service Assistance

With identity theft problems growing, the Service finally established a unit to specifically handle these issues. The new unit is the IRS Protection Specialized Unit and is reached at the Identity Theft Hotline at 1-800-908-4490. If you are unable to work with the unit, or the unit is not properly handling your client's matter, the next place to turn is the Taxpayer Advocate Service, which can be contacted at 1-877-777-4778. The taxpayer should turn to the advocate's office for assistance if the Service has not properly resolved the matter. The advocate's office will assign the case to a specific individual and will make contact for this matter easier.

Before the Service has knowledge of the identity theft activity, there is nothing that it will do to an individual's account to indicate that it could be targeted. Action will occur only after the account actually is targeted. That does not mean that taxpayers should do nothing on their own. A taxpayer can and should be proactive. She can monitor use of her social security number by ordering a free credit report each year and checking for unauthorized activity. While a taxpayer cannot always prevent her identity from being stolen or used in an unauthorized manner, she can work with the Service to resolve the resulting tax problem. ■