Identity Theft and Refund Fraud

Passard C. Dean, DBA, CMA, CFE, CRMA, FLMI
Saint Leo University
USA

Ann Meaders, MAcc
Saint Leo University
USA

Abstract

There are billions of dollars in fraudulent income tax return claims filed every year due to individual(s) intentionally using someone else's personal information in order to file a tax return; resulting in identity theft. These scams are on the rise and auditors have concerns that there are billions more that will remain undetected. Taxpayers who have fallen victim to these scams seek answers from the Internal Revenue Service (IRS) with little direction and months of frustration. Therefore, the taxpayer must remain vigilant, ever maintaining awareness of identity theft, and taking preventative measures to prevent identity theft. The IRS continues modernization efforts to provide the vision of a real-time taxpayer system verses the current looking-back system with the intention of reducing these scams.

Identity Theft According to the IRS

Identity theft within the IRS transpires when an individual uses another person's name, social security number (SSN), and other personal information, without their knowledge, with the express intent to file a fraudulent tax return so as to obtain a fraudulent tax refund or commit additional crimes (IRS, 2013). Identity theft has been on the rise over the past few years, which has resulted in generating over two and a half times the number of fraudulent claims in 2011. In 2011, the number of identity theft incidents was1,125,634 and in 2010 the number of incidents was440,581.The IRS has an identity theft program to prevent, detect, and resolve these cases, however they are not equipped to handle a challenge of this magnitude (McKenney, 2012).

In 2011 alone with over 1.1 million identity theft cases identified, some of the taxpayers were unaware their identity had even been stolen as they were either no longer required to file a tax return or had yet to begin the process to file their return (McKenney, 2012).The primary targets for potential tax refund fraud are social security numbers in several target ranges. They include the social security numbers of deceased individuals; low income families, or elderly persons not required to file income tax returns as they do not meet the income threshold for filing. Another group targeted is students between the ages of sixteen to twenty-two. This is so because many students are not required to file and some do not realize they could file to get a refund. While the aforementioned groups are usually targeted, some victims may never be discovered. These target rich environments are compounded by the IRS's budget constraints; however the IRS has implemented newly designed identity theft screening filters to assist in the identity theft prevention process (McKenney, 2012).

Detect, Prevent, and Resolve

In order to detect identity theft, the IRS with the suggestions of the Treasury Inspector General for Tax Administration (TIGTA) auditors have sought to find more and better ways to prevent identity thieves from receiving fraudulent refunds. The first step towards detection was to increase the number of fraud screening filters in order to detect characteristics of a fraudulent return (McKenney, 2012). If indicators reflect the tax return requires verification from the taxpayer, then an IRS agent attempts to make contact in order to confirm their identity. Generally, this is done either over the telephone or through the mail, never over the Internet. The return's processing is stopped until the taxpayer's identity is confirmed.

This process is used to prevent the issuance of fraudulent refunds and has thus far prevented the issuance of more than $5.2 billion in fraudulent refunds (McKenney, 2012).

The IRS has taken additional efforts to detect and prevent refund fraud. Through a foiled scheme in 2011, several law enforcement agencies uncovered multiple schemes involving fraudulent refunds using the SSN's of descendants and individual's on government assistance. How the SSN's were compromised remains undisclosed. Since this $130 million scheme took place in the Tampa, Florida area, the IRS has embedded a unique identifier on deceased individuals' SSN's to prevent this fraud from being committed in the future (IRS, 2012).

Individuals are responsible for diligently protecting their personal information. This includes, but is not limited to ensuring the security of personal information by keeping one's SSN in a secure place and limiting who it is released to. Individuals who have been involved in the theft of a wallet and/or purse containing their identification documents should notify the IRS to ensure the individual's tax account is not subject to identity theft.

It is imperative that individuals ensure their identities are secure by shredding personal documents prior to their disposal. Precautions should be taken in public surroundings to be aware of who can hear personal conversations with privileged information. During telephone conversations individuals should ensure they do not give personal information unless they are sure they know they are providing it to legitimate sources. That is, they initiated the call or are familiar with the caller. If uncertain, calling back the organization requesting the information using a known number prior to releasing the requested information is a good idea. Another means of protecting sensitive information is to request the individual on the other side of the call to caller to repeat the information as other people may be in the room thus allowing the possibility for theft.

With the wide variety of technology individuals use on a daily basis security is a top priority. The protecting of computer devices using firewalls, anti-spam and anti-virus software with current updates is imperative. All technology should be password protected with an unusual selection of letters (upper and lower case), numbers and other characters to enhance security. Passwords need to be changed periodically to ensure continued security. Additionally, there are fraud monitoring and identity theft insurance services available to purchase which would notify an individual of identity theft and assist in the clean-up from the fraud. However, checking one's credit report every six months or at least annually is very important.

While there is much that can be done to prevent and detect identity theft, it is important to note that these cases are complex, time consuming, and extremely challenging for all parties involved. The initial phase of determining who is the legitimate taxpayer is the most extensive and tedious part of the process. This is so because there are times when it is the result of a transposed SSN or even when the Social Security Office has issued the same SSN twice (IRS, 2013). As a result, victims are affected for multiple years in the tax filing process. To ensure identity theft does not occur in the future, a taxpayer's account has one of six identity theft indicator codes embedded in it by the IRS for future references. In the future returns the taxpayer will have an Identity Protection Personal Identification Number (IP PIN) to uniquely identify the filer and prevent future filing delays (IRS, 2013).

Looking–Back Tax System

The IRS currently operates a "looking-back" system; where information is verified after receipt of the tax return, which opens the door for refund fraud (IRS, 2013). The IRS could be linked to third party databases which would serve as a tool for prevention of refund fraud, even though a great deal of information is unavailable due to tax return filings dates beginning prior to business report filing dates. The National Directory for New Hires (NDNH) database compiles information from the W-4's; the employee's name, up-to-date address, and SSN. However, this information is not available for the IRS to access until a fiscal budget is passed for the IRS, and tax return fraud will continue to rise (IRS, 2013).

Tax refunds can be disbursed in the form of debit cards, electronic transfer of funds into a bank account, or a check by mail. Currently the banking industry has rigorous guidelines to establish one's identity prior to opening a bank account (IRS, 2013). In order to prevent refund fraud these guidelines should be administered to refund disbursements. Additional measures to assist in fraud prevention in 2011 by the TIGTA auditors were recommended restricting the number of deposits being allowed into a single bank account. Direct deposit accounted for eighty-two percent of the 1.5 million tax returns filed (IRS, 2013). Direct deposit eliminates the challenges of trying to cash a paper check.

The matching of a taxpayer to their bank account is another form of identity verification towards fraud deterrence. The most prevalent form of refund fraud used by thieves is debit cards, as most purposely file below the $35,000 income threshold(IRS, 2013).The IRS issues the debit cards through a pilot program to assist taxpayers' who do not have bank accounts. Fraudsters have the ability to purchase anything they choose with these cards and do not have to provide any identity in order to use the money pre-loaded by the IRS from the fraudulent refund amounts (Phillips, 2012). The banking institutions have a basis to establish their customer's identity which the IRS can learn a great deal from along with the recommendations of the TIGTA auditors'.

Modernization

The IRS processes millions of tax returns and must maintain over 178 computer systems in order to satisfy their needs (George, 2013). With all these systems, many locations and employees tasked with maintaining security, it is frustrating since the Department of Homeland Security stated their systems have fallen prey to 43,889 cyber-attacks in 2011. This represented approximately a 5% increase over 2010 (George, 2013).These computers contain vital information on millions of people across the Unites States and the world at large. To state the obvious, these systems have to be monitored continuously in an attempt to secure this data.

For the past fifteen years, the IRS's computer system was stated to be "a material weakness during its annual evaluation of internal accounting and administrative controls under the *Federal Managers' Financial Integrity Act 1982"* (George, 2013). It is expected that modernization will remove this material weakness from the IRS's system. Included in the efforts of modernization is moving to a real-time tax system. However, the budget for this modernization has to be passed.

Real-Time Tax System

Currently the IRS matches tax return data as much as a year, if not more than a year, after the tax return was filed and processed. IRS Commissioner Douglas Shulman stated, "This after-the-fact compliance approach can create problems and frustrations for both taxpayers and the IRS" ("Irs holds first", 2011). The IRS can audit individuals' returns, going back three years, but by then the refund money is no longer available even if it were to have been a legitimate claim with an error. There are visions to create a new real-time tax system. The real-time tax system will make remarkable strides within the U.S. tax system in terms of accuracy, efficiency, and the ability to reduce the taxpayer's burden. With this new system taxpayers are able to correct errors prior to the acceptance of the tax return thus gaining the opportunity to access documents when items are readily available not years later("Irs holds first", 2011). This system has the potential to confirm a taxpayer's income as well as their identity to reduce tax refund fraud.

The IRS has an opportunity to implement the real-time tax system properly. In doing so they would be able to stop inaccurate claims from being processed as well as catching fraud before refunds are issued. This would be a significant improvement for the U.S. tax system; to efficiently and effectively process a tax return both accurately and completely at the time of processing, for the simpler returns. This system would have to start with the individual form 1040's and then progress to business tax forms in the future to ensure accuracy ("Irs holds first", 2011).

Conclusion

The IRS has experienced rising cases of identity theft resulting in refund fraud. Currently due to the "look-back" system the IRS is able to detect, prevent, and resolve only after-the-fact of processing a taxpayer's return. This process makes it is easier for fraudsters to perpetrate fraud. Modernization of the IRS's computer systems is necessary due to the material weakness auditors discovered more than fifteen years ago and could take an additional fifteen years to put in place (George, 2013). Therefore, the vision is to initiate a "real-time" tax system. This would begin with the individual 1040 forms and progress to the business tax forms in the future. The IRS should have access to third party agencies; after all they are government offices. Social Security Office and NDNH should not require law approval for accessing the databases yet it is required (George, 2013).

The vision is very simple. The real-time tax system for the IRS would allow access to all third party information prior to processing tax returns, thereby enabling errors to be corrected prior to processing and vastly reducing identity theft fraud on tax returns. This will result in changes for the taxpayer, the preparer, and the IRS, however, in this case change is good.

References

George, J. R. Department of Treasury, (2013).*Management and performance challenges facing the internal revenue service for fiscal year 2013*(2012-40-050). Retrieved from website: http://www.treasury.gov/tigta/management/management_fy2013.pdf

IRS. U.S. Department of Treasury, Internal Revenue Service. (2013). *Irs intensifies national crackdown on identity theft; part of wider effort to protect taxpayers, prevent refund fraud* (IR-2013-17). Retrieved from website: http://www.irs.gov/uac/Newsroom/IRS-Intensifies-National-Crackdown-on-Identity-Theft-January-2013

McKenney, M. E. Chairman of the Senate Finance Committee, Subcommittee on Fiscal R, and (2012) .Final *audit report – There are billions of dollars in undetected tax refund fraud resulting from identity theft* (201140044). Retrieved from website: http://www.treasury.gov/tigta/auditreports/2012reports/201242080fr.html

(n.d.). Irs holds first hearing on real-time tax system. (2011).*Journal of Accountancy*, Retrieved from http://www.journalofaccountancy.com/Web/20114879

Phillips, M. R. Treasury Inspector General for Tax Administration, Internal Revenue Service Deputy Commissioner for Operations Support. (2012).*Final audit report – most taxpayers whose identities have been stolen to commit refund fraud do not receive quality customer service*(2012-40-050). Retrieved from Washington, D.C. website:

http://www.treasury.gov/tigta/auditreports/2012reports/201240050fr.html