INTER- AMERICAN CENTER OF TAX ADMINISTRATIONS

48ª. GENERAL ASSEMBLY

THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN THE TAX ADMINISTRATION

Subtopic 3.2

IDENTITY THEFT: CHALLENGES AND OPPORTUNITIES

Internal Revenue Service
USA

May 5 - 8, 2014
Rio de Janeiro, Brazil

Identity Theft

Summary: Although the problem of identity theft is not new, the increasing use of the internet to perform day to day activities has increased the opportunities to both steal and use identification information. While the internet makes it possible to quickly file a legitimate tax return and have a tax refund deposited in a bank account, it also makes it possible to quickly file a fraudulent tax return and receive a tax refund. The Internal Revenue Service (IRS) recognizes that identity theft is an important concern to all taxpayers, and its employees are addressing the problem on many fronts. As a result of its aggressive efforts to combat identity theft, the IRS stopped 14.6 million suspicious returns and protected over $50 billion in fraudulent refunds from 2011 through November 2013.

The IRS has over 3,000 employees focused solely on identity theft issues. The IRS investigates identity theft cases and prosecutes identity thieves. The IRS works to prevent refund fraud by educating taxpayers to take actions that minimize third-party access to social security numbers, by expanding the number of identity theft filters used to recognize patterns in fraudulent returns, by increasing monitors and controls over direct deposits of refunds to bank accounts or debit cards, and by trying to match third-party information reporting and tax return reporting at an earlier stage of tax return processing. The IRS investigates identity theft-related crimes and uses centralized data bases, from both within the IRS and with other governmental agencies. It helps taxpayers who have been victimized by identity thieves by sharing taxpayer information with other law enforcement agencies to expand the network tracking the thieves and by providing a special identity number to taxpayers who have been the victim of identity theft so the IRS recognizes their return as legitimate. The IRS continues to dedicate more and more employees to the resolution of cases involving victims of identity theft. The IRS has developed, and continues to develop, methods to identify fraudulent returns and refunds earlier, so that it can prevent the returns and refunds from being processed.

Many groups, both within the IRS and from other government agencies, address the problem of identity theft. Oversight groups review IRS actions and recommend additional or different steps that the IRS can take to improve its ability to detect identity theft and prevent refund fraud.

I. A Brief History of Identity Theft

Identity theft is not a new phenomenon. If you search for “Identity Theft” on the internet, one hit states that the first case of identity theft occurred in the book of Genesis in the Bible, when Jacob covered himself in skins to fool his father into thinking that Jacob was his brother Esau. As a result of this identity theft, Jacob obtained his father’s blessing and all the sheep and lands that really belonged to Esau.[1]

[1] http://idtheft.about.com/od/identitytheft101/a/A-Brief-History-Of-Identity-Theft.htm, referring to Genesis, chapter 27

Identity theft has diverse purposes. When the drinking age is 21, many young people acquire identification cards that indicate they are someone else or at least older than they really are. People have false or alternate identification for voter fraud and other types of identity fraud.[2]

The age of the internet has expanded both the ability to steal someone's identity and the ability to use that stolen identity. Hackers access seemingly secure sites and take social security and credit card information, which they then use to purchase items or, in more complex situations, apply for more credit cards. This leaves the actual owner of the identity liable for unknown financial charges and facing what may be months or years of effort to undo the effect of the theft.[3]

There was no federal law making identity theft a crime until 1998.[4] At that time, the Federal Trade Commission (FTC) was tasked with establishing procedures to keep track of instances of identity theft, inform people about identity theft, and take appropriate actions about identity theft.[5] Accounting for more than 43 percent of the FTC's identity theft complaints in 2012, tax identity theft was the largest category of identity theft complaints by a substantial margin. In addition, the percentage of tax identification theft complaints nearly doubled, from just over 24 percent in 2011.[6] The FTC has reported identity theft as the number one consumer complaint since calendar year 2000.[7] Clearly this is a problem that is not going away.

II. Types of Identity Theft

Identity theft occurs when someone wrongfully obtains and uses another person's personal data in a way that involves fraud or deception, typically for economic gain.[8] There are many types of identity theft. Financial identity theft includes both the theft of credit card information and the theft of a social security number (SSN). Criminal identity theft occurs when someone wants to be a different person, for whatever reason. Driver's license identity theft occurs to provide drivers' licenses for individuals not otherwise able to get a license, whether the reason is because the person simply needs to be able to drive or because the person wishes to enter or remain illegally in the United States. Medical identity theft involves the theft of identification to obtain medical care or services.[9]

When an identity thief steals a credit card or credit card number, the thief takes over the identity of the victim and obtains new credits cards or uses stolen credit cards to buy goods and services. This type of identity theft has been prominent recently with reports about the massive identity thefts that occurred at Target stores in November and

[2] Id.
[3] Treasury Inspector General for Tax Administration (TIGTA), Ref. No. 2005-40-106, *A Corporate Strategy Is Key to Addressing the Growing Challenge of Identity Theft* (July 2005), p. 1
[4] *See* PL 105-318, The Identity Theft and Assumption Deterrence Act of 1998
[5] Id., sec. 5
[6] http://www.ftc.gov/news-events/press-releases/2014/01/ftcs-tax-identity-theft-awareness-week-offers-consumers-advice
[7] TIGTA, Ref. No. 2013-40-122, *Detection Has Improved; However, Identity Theft Continues to Result in Billions of Dollars in Potentially Fraudulent Tax Refunds* (September 20, 2013), p. 1
[8] http://www.justice.gov/criminal/fraud/websites/idtheft.html
[9] http://www.consumer.ftc.gov/features/feature-0014-identity-theft

December 2013,[10] as well as at Neiman Marcus.[11] In some cases, the victim does not learn of credit card theft until substantial damage is done – the credit card companies go after the victim for payment of the charges under the credit card and their credit scores decline. Credit card companies are trying to address this problem in many ways, including through the use of a chip imbedded in the credit card.[12]

The theft of an SSN is the second type of financial identity theft. There are two primary types of SSN identity theft that relate to tax administration. One type involves using another person's identity (name, SSN, or both) to obtain employment. The second type involves using another person's identity (name and/or SSN) to file a fraudulent tax return to unlawfully obtain a tax refund.[13]

Identity theft for employment purposes generally involves the theft of a single identity. The thief could be an individual who is in the United States (legally or illegally) without authorization to work, but who wants to work, or he or she could be someone who is trying to escape a real financial past – perhaps the individual has prior debts or child support payments and wants to remain hidden in the United States. In either case, the individual steals an SSN number[14] and presents him or herself to an employer as an individual able to work in the United States with this specific SSN. The employer relies on this valid SSN – although not valid for this individual – and hires the individual, withholding and remitting taxes to the federal government on the income paid to the individual. The employer reports the income and taxes on a W-2. While the identity thief often does not file a tax return, the individual who is the lawful owner of the SSN does file a tax return to report wages, other income, and withheld taxes. The individual has no knowledge of the income earned by the identity thief, so he does not include these wages in income. In its matching process, the IRS associates two W-2's with one SSN and contacts the legal owner of the SSN to increase reported income and request additional taxes.[15] Then the individual has the difficult challenge of providing a negative – he or she did not perform the work and receive the wages, even though the W-2 issued by the employer indicates that the work was performed. The Treasury Inspector General for Tax Administration (TIGTA) reviewed the IRS' actions in assisting victims of identity theft in 2008. It determined that, while the IRS had made progress in addressing employment-related identity theft, substantial work was still needed. Most IRS efforts at that time were related to outreach and not to the prosecution of identity theft cases.[16]

Perhaps the more costly type of identity theft to the IRS is identity theft that results in refund fraud. In this type of identity theft, the thief steals a number of SSNs and files fraudulent tax returns to claim refunds. Even if the IRS detects this fraud during its

[10] http://www.nytimes.com/2013/12/20/technology/target-stolen-shopper-data.html?pagewanted=all&_r=0
[11] http://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html
[12] http://www.usatoday.com/story/news/nation/2014/01/09/encrypted-chips-help-fight-credit-card-fraud/4400347/
[13] TIGTA, Ref. No. 2005-40-106, pp. 5 - 6
[14] It is not even necessary to steal an SSN. Some people buy real or counterfeit SSNs. See http://oig.ssa.gov/what-abuse-fraud-and-waste/buying-or-selling-counterfeit-or-legitimate-social-security-cards.

[15] TIGTA, Ref. No. 2005-40-106, p. 6
[16] TIGTA, Ref. No. 2008-40-086, *Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft* (March 25, 2008), p. 2

review process, it faces the lengthy and costly task of pursuing the thief to recoup any refunds made.

The methods of stealing a person's identity (usually the SSN and/or name) are numerous and often occur in connection with the identity thief's regular employment. Recent cases about identity theft include the following:

1. 2 corrections officers in Alabama with access to the personal identifying information of every inmate in the custody of the Alabama Department of Corrections, past and present, used information stolen from the databases to file false federal income tax returns in the names and SSNs of inmates. They directed stolen tax refunds onto prepaid debit cards and requested other refunds in the form of U.S. Treasury Checks.[17]
2. In three different cases, workers at nursing homes used their positions to obtain personal identifying information from thousands of patients. With the help of others, that information was used to submit fraudulent federal tax returns and receive tax refunds in the patients' names.[18]
3. A clerk of court had access to the Florida Department of Highway Safety and Motor Vehicle Driver and Vehicle Information Database. The clerk copied personal identity information and provided the information to a co-conspirator in exchange for a cash payment. The information was used to file fraudulent tax returns seeking refunds.[19]
4. A part-time IRS data entry clerk stole tax returns from the IRS Service Center where she worked and filed fraudulent tax returns using information from the stolen tax returns to claim excessive federal tax withholdings.[20]
5. An IRS tax examining technician was recently indicted (formally accused but not yet tried) for identity theft. The employee had access to taxpayer personal identifying information as part of her job and shared it with co-conspirators to file fraudulent tax returns requesting refunds. She then used her access to IRS computers to review these fraudulent returns and authorize the release of the refunds.[21]
6. Two individuals in Alabama filed over 500 fraudulent tax returns seeking at least $3.7 million in tax refunds. The individuals fraudulently obtained the names and SSNs of Medicaid beneficiaries through the employment by one of the individuals at a company that services Medicaid programs.[22]

[17] http://www.justice.gov/opa/pr/2014/January/14-tax-084.html.
[18] http://www.fbi.gov/atlanta/press-releases/2014/yolando-blount-sentenced-to-27-years-in-nursing-home-identity-theft-scheme;http://www.justice.gov/opa/pr/2014/January/14-tax-048.html; http://www.justice.gov/usao/vae/news/2014/01/20140124ighalonr.html.
[19] http://www.justice.gov/usao/fls/PressReleases/140117-03.html.
[20] http://www.justice.gov/usao/cae/news/docs/2014/2014_01/01-21-14Hernandez.html.
[21] http://www.treasury.gov/tigta/oi_highlights.shtml.
[22] http://www.justice.gov/opa/pr/2011/October/11-tax-1366.html

No one is immune from being a victim of identity theft. An individual was recently found guilty of the theft of the identities of more than ten individuals, including the United States Attorney General.[23]

III. Factors Contributing to the Growth in Identity Theft

1. The Internet

When everyone kept their identification information in their wallet or desk and shared it only by showing it to someone, identity theft could occur only if an individual physically showed the information to a third party or if the identification card was lost or stolen. The increasing popularity of the Internet is making the personal exchanges of information almost nonexistent. Instead, people buy goods and services online and pay for them with credit card information provided online. They may even provide substantial personal identification information – birthday, SSN, etc. – online in connection with a purchase or other activity. Even moderately skillful hackers can access this information and use it for illegal purposes. The "personal" filter of face to face interaction no longer works to detect fraud.

2. Competing Goals at the Internal Revenue Service

a. Electronic return filing

Title II of the Internal Revenue Service Restructuring and Reform Act of 1998 provided that it was Congress's policy that the electronic filing of federal tax and information returns was the preferred means of filing returns and that it was the goal to have 80 percent of all returns filed electronically by 2007.[24] Thus, the IRS had the mission of facilitating tax return filing through the internet.

b. Quick refunds

The taxpayer always wants her tax refund as soon as possible. Certain credits, such as the Earned Income Tax Credit, are made available only as a refund after a tax return is filed. Returns are filed electronically and taxpayers want a refund immediately. Refunds made by direct deposit into a checking or savings account are available to the taxpayer more quickly than refunds made than with a paper check.[25] As a result, returns are received and refunds are processed well before the return is screened for accuracy (other than for the standard math and other simple errors). In addition, while a human reviewing return might have noticed without prompting a pattern of multiple refunds being mailed to the same address, computers must be programmed to identify specific issues.

---

[23] http://www.fbi.gov/atlanta/press-releases/2014/identity-thief-sentenced-for-filing-tax-returns-in-the-names-of-the-attorney-general-and-others

[24] Pub. L. 105-206, sec. 2001. This goal was achieved for filing year 2012. http://www.irs.gov/uac/2012-Filing-Season-Statistics.

[25] 2013 Instructions for Form 1040, Individual Income Tax Return, p. 69.

c. Lack of centralization

Many groups at the IRS are involved in one or more aspects of the identity theft process. The National Taxpayer Advocate has identified almost 20 different units at the IRS that could be involved in resolving an identity theft issue and has criticized the IRS for not having one central contact per victim.[26] This contact would make sure that all groups that need to be involved are involved, without having each group treat the same identity theft event as a new issue. It may take 20 months – or even longer – before issues relating to identity theft are resolved.[27] TIGTA identified as an issue in the investigation of a large refund fraud scheme the fact that confiscated mail was being worked by multiple functions within the IRS. This makes it difficult to track issues such as multiple deposits to the same account or to identity large patterns of behavior.[28]

IV. Addressing Identity Theft

A. Oversight and Recommendations

The National Taxpayer Advocate has identified issues relating to identity theft as one of the Most Serious Problems in the Annual Report submitted to Congress in nearly every year since 2003.[29] The Government Accountability Office (GAO) first considered identity theft (referred to as "identity fraud") in a report issued in 1998.[30] Four years later it reported that all measures available indicated that the prevalence of identity theft was growing.[31] In 2009 GAO assessed the IRS's efforts to address the impact of identity theft on taxpayers, including efforts to prevent and detect identity theft-related tax problems[32] and has continued to review IRS initiatives and actions in recent years.[33] TIGTA first considered identity theft in a report issued in 2005[34] and has revisited specific issues relating to identity theft in many reports issued since 2005. It has

---

[26] http://www.taxpayeradvocate.irs.gov/userfiles/file/2013FullReport/IDENTITY-THEFT-The-IRS-Should-Adopt-a-New-Approach-to-Identity-Theft-Victim-Assistance-that-Minimizes-Burden-and-Anxiety-for-Such-Taxpayers.pdf.

[27] TIGTA, Ref. No. 2012-40-050, *Most Taxpayers Whose Identities Have Been Stolen to Commit Refund Fraud Do Not Received Quality Customer Service* (May 3, 2012), p. 8

[28] TIGTA, Ref. No. 2012-42-080, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft* (July 19, 2012), p. 17

[29] See., e.g., http://www.irs.gov/pub/irs-utl/nta_2003_annual_update_mcw_1-15-042.pdf (discussing identity theft where undocumented workers uses stolen SSNs to obtain employment); http://www.irs.gov/pub/tas/ntafy2004annualreport.pdf (identity theft treated differently at different IRS campuses); http://www.irs.gov/pub/irs-utl/section_1.pdf (2005 Most Serious Problem #9 is *Identity Theft*); http://www.irs.gov/pub/tas/arc_2007_vol_1_cover_msps.pdf (2007 Most Serious Problem #6 is *Identity Theft Procedures*); http://www.irs.gov/pub/tas/irs_tas_arc_2011_vol_1.pdf (2011 Most Serious Problem # 3 is *Tax-Related Identity Theft Continues to Impose Significant Burdens on Taxpayers and the IRS);* http://www.taxpayeradvocate.irs.gov/userfiles/file/2013FullReport/IDENTITY-THEFT-The-IRS-Should-Adopt-a-New-Approach-to-Identity-Theft-Victim-Assistance-that-Minimizes-Burden-and-Anxiety-for-Such-Taxpayers.pdf (2013 Most Serious Problem #6)

[30] GAO/GGD-98-100BR, *Identity Fraud: Information on Prevalence, Cost, and Internet Impact is* Limited (May 1998)

[31] GAO-02-363, *Identity Theft: Prevalence and Cost Appear to be Growing* (March 2002)

[32] GAO-09-882, *Tax Administration: IRS Has Implemented Initiatives to Prevent, Detect, and Resolve Identity Theft-Related Problems, but Needs to Assess Their Effectiveness* (September 2009)

[33] GAO-13-515, *Tax Refunds: IRS is Exploring Verification Improvements, but Needs to Better Manage Risks* (June 2013). Officials at GAO also have testified before Congress on issues related to identity theft. See GAO-11-721T, *Taxes and Identity Theft: Status of IRS Initiatives to Help victimized Taxpayers*, Testimony of James R. White Director Strategic Issues, before the Subcommittee on Government Organization, Efficiency and Financial Management, Committee on Oversight and Government Reform, House of Representatives (June 2, 2011) and GAO-12-132T, *Identity Theft: Total Extent of Refund Fraud Using Stolen Identities is Unknown*, Testimony of James R. White Director Strategic Issues, before the Subcommittee on Government Organization, Efficiency and Financial Management, Committee on Oversight and Government Reform, House of Representatives (September 29, 2012)

[34] TIGTA, Ref. No. 2005-40-106

recommended actions to help minimize the incidence of identity theft or resolve issues relating to individual identity theft more quickly.[35]

In 2005, TIGTA made five recommendations to the IRS to help address their determination that the IRS had no corporate strategy to address identity theft issues or centralized data on identity theft: (1) ensure agency-wide communication tools are updated to include information about identity theft, (2) ensure information provided by the IRS to taxpayers or for use by other Federal Government agencies when referring individuals to the IRS is complete and accurate, (3) develop agency-wide standards to ensure consistency when requiring taxpayers to substantiate claims and when allowing taxpayers future exemptions and credits, (4) develop specific closing codes for cases involving identity theft, and (5) develop an Enterprise Identity Theft Strategy that includes processes to proactively identify instances of identity theft and to resolve identification number discrepancies, while protecting tax revenue and enforcing the law.[36] In October 2005, the IRS established the Identity Theft Program to develop centralized policy and procedural guidance.[37] TIGTA acknowledged in its 2008 report that the IRS had made progress in the implementation of these recommendations, but it identified other areas for improvement. TIGTA has continued to review identity theft in audit reports and has testified before Congress.[38]

B. Increased Participation of Criminal Investigation

As of 2013, identity theft-related crimes are a priority area of investigation for the Criminal Investigation Division (CI) within the IRS.[39] In its 2013 Annual Report, CI indicated that it participates in over 70 task forces/working groups throughout the country that investigate both financial crimes as well as identity theft crimes.[40]

The investigative work done by CI is a major component of the IRS's efforts to combat tax-related identity theft. The IRS has seen a significant increase in refund fraud that involves identity thieves who file false claims for refunds by stealing and using someone's SSN. In the most recent fiscal year (October 1, 2012 through September 30, 2013), the IRS initiated approximately 1,492 identity theft related criminal investigations, an increase of 66 percent over investigations initiated in FY 2012.[41] Only 276 identity theft related criminal investigations were initiated in FY 2011. Direct investigative time

---

[35] See, e.g., TIGTA, Ref. No. 2008-040-086; TIGTA Ref. No. 2012-40-050; TIGTA Ref. No. 2012-42-080; TIGTA Ref. No. 2013-40-062, *The Tax Protection Program Improves Identity Theft Detection; However, Case Processing Controls Need to be Improved* (June 21, 2013); TIGTA 2013-40-122

[36] TIGTA Ref. No. 2005-40-106, pp. 12 – 20.

[37] TIGTA Ref. No. 2008-40-086, p. 3

[38] See, e.g., Testimony of The Honorable J. Russell George, Treasury Inspector General for Tax Administration, *Identity Theft and Tax Fraud*, before the Committee on Oversight and Government Reform, Subcommittee on Government Organization, Efficiency and Financial Management (November 4, 2011); Testimony of The Honorable J. Russell George, Treasury Inspector General for Tax Administration, *Identity Theft and Tax Fraud: Growing Problems for the Internal Revenue Service, Part IV*, before the Committee on Oversight and Government Reform, Subcommittee on Government Organization, Efficiency and Financial Management (November 29, 2012); Testimony of Michael E. McKenney, Acting Deputy Inspector General for Audit, Treasury Inspector General for Tax Administration, *Refund-Related Identity Theft*, before the Committee on Oversight and Government Reform, Subcommittee on Government Operations (August 2, 2013)

[39] http://www.irs.gov/pub/foia/ig/ci/REPORT-fy2013-ci-annual-report-02-14-2014.pdf, p. 7

[40] http://www.irs.gov/pub/foia/ig/ci/REPORT-fy2013-ci-annual-report-02-14-2014.pdf, p. 7. As recently as 2008, TIGTA noted that IRS policy was that the actual crime of identity theft would only be investigated by CI if it was committed in conjunction with other criminal offenses having a large tax effect. TIGTA, Ref. No. 2008-40-086, p. 5

[41] http://www.irs.gov/pub/foia/ig/ci/REPORT-fy2013-ci-annual-report-02-14-2014.pdf, p. 10

applied to identity theft related investigations has increased 216 percent over the last two years. Prosecution recommendations, indictments, and those convicted and sentenced for identity theft violations have increased dramatically since FY 2011. Sentences handed down for convictions relating to identity theft have been significant, ranging from two months to 317 months.

CI has many tools and methods to stop identity theft. Some of them include the following.[42]

1. Identity Theft Enforcement Sweeps - In January 2013, CI conducted a coordinated identity theft enforcement sweep in collaboration with the Department of Justice-Tax and United States Attorney's Offices throughout the country.[43] This nationwide effort resulted in 734 enforcement actions related to identity theft and refund fraud and involved 389 individuals, 109 arrests, 48 search warrants, and 189 indictments, information and criminal complaints. This continued the coordinated enforcement efforts begun earlier.[44]

2. Law Enforcement Assistance Program - In March 2013, IRS announced that the Law Enforcement Assistance Program, formerly known as the Identity Theft Pilot Disclosure Program, was expanded nationwide.[45] This program provides for the disclosure of federal tax return information associated with the accounts of known and suspected identity victims of identity theft. With the express written consent of the victim of identity theft, the IRS releases the fraudulent tax return information filed by the identity thief to the law enforcement agency. There are currently more than 300 state/local law enforcement agencies from 35 states participating in the program. The Law Enforcement Assistance Program includes all 50 states, the District of Columbia, and U.S. territories.[46] As of May 30, 2013, the IRS has processed 2,731 waivers from 244 different law enforcement agencies.[47]

3. Identify Theft Clearinghouse - CI established the Identity Theft Clearinghouse (Clearinghouse) in 2012 to provide it with a central location to review and process identity theft leads.[48] The Clearinghouse performs research on each lead to develop it for the field offices and ensure that an open investigation is not already underway. In addition, the Clearinghouse analyzes characteristics of identity theft from fraudulent refund claims and passes relevant information to the appropriate function to attempt to incorporate newly identified fraud characteristics into identity theft filters.[49] For FY 2013, the ITC received over 1,400 identity theft related leads. Those leads related to more

[42] http://www.irs.gov/uac/Newsroom/IRS-Criminal-Investigation-Combats-Identity-Theft-Refund-Fraud.
[43] http://www.irs.gov/uac/Newsroom/IRS-Intensifies-National-Crackdown-on-Identity-Theft-January-2013.
[44] http://www.irs.gov/uac/Identity-Theft-Crackdown-Sweeps-Across-the-Nation;-More-than-200-Actions-Taken-in-Past-Week-in-23-States.
[45] http://www.irs.gov/uac/Law-Enforcement-Assistance-Pilot-Program-on-Identity-Theft-Activity-Involving-the-IRS; http://www.irs.gov/uac/Newsroom/IRS-Combats-Identity-Theft-and-Refund-Fraud-on-Many-Fronts-2014.
[46] TIGTA Ref. No. 2013-40-122, p. 5
[47] Testimony of Michael E. McKenney, footnote 38, p. 3
[48] TIGTA recommended that the IRS develop processes to analyze identity theft characteristics in 2012. TIGTA, Ref. No. 2012-42-080, p. 12
[49] TIGTA, Ref. No. 2013-40-122, p. 5

than 391,000 tax returns claiming in excess of $1.3 billion dollars in potentially fraudulent federal income tax refunds.[50]

The Clearinghouse is similar to the Identity Theft Data Clearinghouse maintained by the Federal Trade Commission, which is the nation's repository for identity theft complaints and a part of the FTC's Consumer Sentinel Complaint database. It offers more than 2,000 law enforcement agencies a variety of tools to facilitate the investigations and prosecutions of identity theft.[51]

4. Data Processing Center (DPC) Identity Theft Victims List Process - This process centralizes identity theft victims' lists and information forwarded to CI by other federal, state and local agencies during nationwide investigative efforts. The information is analyzed and necessary adjustments are made to accounts of taxpayers that are likely targets of ID theft. The DPC processed over 71.7 percent more identity records in FY 2013 than it did in FY 2012.[52]

C. Monitoring Direct Deposit Accounts

In an effort to decrease the length of time between filing a tax return and receiving the associated refund, the IRS provides for the direct deposit (which includes deposits to accounts linked to debit cards) of a refund rather than mailing a paper check.[53] Taxpayers provide a routing and bank account number, as well as the type of bank account, on the return, and any refund is directly deposited into that bank account.[54]

Unfortunately, however, direct deposit also offers criminals the ability to quickly receive fraudulent tax refunds without the challenge of negotiating a tax refund paper check.[55] Limiting the number of tax refunds that can be directly deposited to the same tax account could minimize losses associated with fraud. Federal direct deposit regulations require that deposits be made only to an account in the name of the filer.[56] In 2008 TIGTA indicated that the IRS had not developed processes to ensure that the more than 61 million Filing Season 2008 tax refunds were deposited only to an account in the taxpayer's name.[57] TIGTA also identified as an issue the direct deposit of multiple refunds to the same bank account.[58] While the IRS acknowledged that this was an issue, it also indicated that there could be legitimate reasons for multiple deposits, such as multiple owners of the same account.[59]

---

[50] http://www.irs.gov/uac/Newsroom/IRS-Combats-Identity-Theft-and-Refund-Fraud-on-Many-Fronts-2014
[51] http://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security
[52] http://www.irs.gov/uac/Newsroom/IRS-Criminal-Investigation-Combats-Identity-Theft-Refund-Fraud
[53] The 2013 Instructions for Form 1040, Individual Income Tax Return, indicate that one benefit of direct deposit is "You get your refund faster by direct deposit than you do by check." p. 69
[54] In fact, taxpayers can file Form 8888, Allocation of Refund (Including Savings Bond Purchases), and have the refund deposited in up to 3 separate accounts or used to purchase U.S. Savings Bonds
[55] TIGTA, Ref. No. 2008-40-182, *Processes Are Not Sufficient to Minimize Fraud and Ensure the Accuracy of Tax Refund Direct Deposits* (September 25, 2008), p. 7
[56] 31 CFR s. 210.5(a)
[57] TIGTA, Ref. No. 2008-40-182, p. 6
[58] Id, p. 8
[59] Id., p. 12

Four years later, TIGTA reported that the IRS still was directly depositing multiple tax refunds to the same bank account, and it identified 10 instances from the 2010 filing year where the IRS deposited more than 300 refunds to the same account.[60] The inability of the IRS to ensure the accuracy of direct deposit account information continues to be a factor in the ease with which individuals can receive fraudulent tax refunds. In testimony before a House of Representatives subcommittee at the end of 2012, the then-Deputy Commissioner for Operations Support noted that the IRS has a dual mission with refunds and that the IRS must "consider the need to distribute refunds in a timely manner while also ensuring that taxpayer rights [are] protected."[61] In a 2013 report, TIGTA identified 1.2 million undetected Tax Year 2011 tax returns that were potentially fraudulent[62] and found that 1 million (84 percent) of the tax returns used direct deposit to obtain tax refunds totaling approximately $3.5 billion.[63] TIGTA again recommended that the IRS limit the number of tax refunds being sent to the same account. As TIGTA had indicated in a 2012 report, if a limit were in place, the remaining tax refunds would be converted to a paper refund check and sent to the taxpayers. While it is possible that a paper tax refund check could be sent to the identity thief, converting the paper check is more difficult than withdrawing a direct deposit. To cash a check, individuals usually have to provide picture identification matching the name on the tax refund check, in this case the name of the legitimate taxpayer. This means that the identity thief would need to obtain false identification to cash the fraudulently obtained tax refund check. This serves as another deterrent to fraud.[64]

The IRS is taking steps to address these concerns. The Return Integrity and Correspondence Services (RICS) within the Wage & Investment Division is comprised of organizations that strengthen revenue protection and pre-refund compliance, administer refundable credits and provide oversight of content for all notices and letters sent to taxpayers.[65]

RICS' Accounts Management Taxpayer Assurance Program has a process in which it works with banks to obtain information on questionable tax refunds. The process relies on the banks to provide the IRS the information needed to identify tax refunds deposited to debit cards. One bank associated with an identity theft scheme provided the IRS with a list of 60,000 bank accounts, including debit card accounts, it had identified nationwide with questionable tax refunds. The bank intercepted and prevented questionable refunds totaling $164 million from being deposited into these accounts.[66]

[60] TIGTA, Ref. No. 2012-42-080, p. 16. 590 refunds in the total amount of $909,267 were made to one bank account.
[61] Testimony of Beth Tucker, Deputy Commissioner for Operations Support, before the House Committee on Oversight and Government Reform, Subcommittee on Government Organization, Efficiency and Financial management, November 29, 2012, p. 1
[62] These "undetected" returns were identified by TIGTA as having the same characteristics as IRS-confirmed identity theft returns. TIGTA Ref. No. 2013-40-122, p. 3
[63] Id., p. 18
[64] TIGTA, Ref. No. 2012-42-080, p. 15
[65] http://www.irs.gov/uac/Wage-&-Investment-Division-At-a-Glance
[66] TIGTA, Ref. No. 2012-42-080, p. 17

The IRS implemented a program last year that allows financial institutions to reject direct deposit tax refunds based on mismatches between the account name and the name on the tax return. As of September 30, 2013, financial institutions had returned 20,051 refunds totally more than $66 million.[67]

The IRS is still considering how to balance the legitimate needs of multiple owners of the same bank account to receive direct deposit and the illegitimate desire of participants in refund fraud schemes to have multiple deposits made to their accounts. The IRS has developed a filtering tool that groups tax returns based on address, zip code, and/or bank routing number. The groupings are then filtered to identity potentially fraudulent tax returns. As of September 26, 2013, the IRS had identified 267,838 tax returns using these filters and prevented approximately $817 million tax refunds from being issued.[68]

D. IRS Identity Theft Indicator Codes.

Identity theft indicator codes were developed to centrally track identity theft incidents. They are input to the affected taxpayer's accounts.[69] The IRS looks for identity theft, and its efforts have increased the number of cases identified. For example, while taxpayers self-identified only 110,750 incidents of identity theft for calendar year 2011, the IRS identified 1,014,884 incidents of identity theft.[70] Nevertheless, TIGTA has reported that the IRS is still missing many cases of identity theft. For tax year 2010, for example, TIGTA determined that the IRS missed 1.5 tax returns claiming fraudulent refunds in the amount of $5.2 billion; over 5 years, this could result in $21 billion of fraudulent refunds.[71]

The IRS continues to use identity theft indicator codes on taxpayer accounts to avoid sending a refund to an identity thief. After a recent TIGTA audit reporting that indicator codes are not always used when they should be, the IRS agreed to refine its procedures to ensure that appropriate indicators are recorded on taxpayer accounts to document both the opening and closing of identity theft investigations.[72]

[67] Testimony of J. Russell George, Treasury Inspector General for Tax Administration, *Oversight Hearing – Internal Revenue Service*, before the Committee on Appropriations, Subcommittee on Financial Services and General Government, U.S. House of Representatives (February 26, 2014), at http://docs.house.gov/meetings/AP/AP23/20140226/101771/HHRG-113-AP23-Wstate-GeorgeJ-20140226.pdf, p. 17
[68] Id.
[69] Testimony of Michael E. McKenney, footnote 38, p. 4
[70] TIGTA Ref. No. 2012-42-080, p. 1
[71] Id., p. 3. Although the IRS agreed that it is missing cases, it identified actions that had been taken to reduce the number of cases and did not agree that $21 billion was an accurate number. Id., p. 29
[72] TIGTA, Ref. No. 2013-40-062, p. 7 and p. 17

E. Social Security Master Death File

A successful identity theft scheme usually requires an SSN.[73] Thieves steal these SSNs in a variety of ways.[74] One way is to read the Social Security Death Master File daily and take note of the SSNs of individuals who have died. The thieves then file a tax return early in the filing season and show a refund due. When the surviving spouse or executor of the estate files a return requesting a refund, the IRS notifies this individual that this is a duplicative return and that a refund has already been issued. Thieves also use the SSN of infants who have died to file claims for dependent exemptions and other credits.[75]

In 1980, the SSA agreed to release death information following a Freedom of Information Act lawsuit.[76] Information from the Death Master File is available to purchase online through the Department of Commerce. The database contains much of the information needed to steal someone's identity: the full name, SSN, date of birth, and date of death of deceased citizens and legal residents. While the information has important legitimate users – such as the financial community, insurance companies, security firms, and state and local governments - it has also allowed criminals to file fraudulent tax returns.[77]

The Bipartisan Budget Act of 2013 contains a provision to restrict the disclosure of information from the Death Master File for 3 calendar years beginning on the date of death, unless the person has been certified to receive the information.[78] The hope and expectation is that this will prevent any use of SSNs of recently deceased individuals for refund fraud.[79]

In a recent hearing of the House Appropriations Committee, it was noted, however, that the Death Master Files are still open and available for use by anyone, because the National Technical Information Service, which is responsible for maintaining the database, said it does not want to close off the file before making sure that organizations with a legitimate need still have access.[80]

---

[73] An SSN is not required, however. Beginning in 2013, TIGTA identified cases of tax refund fraud using Individual Taxpayer Identification Numbers (ITIN), and determined that there were more than 141,000 Tax Year 2011 returns files with an ITIN that have the same characteristics as IRS-confirmed identity theft tax returns involving an ITIN. TIGTA, Ref. No. 2013-40-122, p. 3

[74] Examples of ways thieves steal SSNs were provided in Section II., Types of Identity Theft.

[75] See, e.g., the National Taxpayer Advocate's Legislative Recommendation #2 for 2011, Restrict Access to the Death Master File, at http://www.irs.gov/pub/tas/2011_arc_legrecommendations.pdf and http://www.wnem.com/story/24781871/stranger-steals-dead-babys-social-security-number-to-file-taxes for a recent case where this happened.

[76] Perholtz v. Ross, Civil Action No. 78-2385 and 78-2386, U.S. District Court for the District of Columbia (Apr. 11, 1980)

[77] http://www.casey.senate.gov/newsroom/releases/budget-deal-contains-casey-backed-plan-to-crackdown-on-identity-theft

[78] Pub. L. No. 113-67, sec. 203

[79] http://www.casey.senate.gov/newsroom/releases/budget-deal-contains-casey-backed-plan-to-crackdown-on-identity-theft

[80] http://www.usatoday.com/story/news/politics/2014/02/06/anti-fraud-efforts-stalled-as-death-master-file-lives-on/5231223/

F. Tax Return Filters

The IRS has achieved the 1998 goal of receiving at least 80% of returns electronically.[81] When these returns are being processed, the IRS runs the returns through a variety of filters that help identify returns that may be involved in refund fraud. The IRS recently announced that for filing year 2014, it will increase both the number and efficiency of the identity theft filters that are used to identity potentially fraudulent returns due to identity theft prior to the processing of the return and release of any refund.[82] In 2012, TIGTA identified a number of returns that the IRS has sent through its filtering process where the return did not score high enough for a more thorough exam.[83] TIGTA indicated that if the IRS had more filters, then returns might score higher on the identity theft scale and result in more scrutiny and reduced refunds. It noted that the IRS increased the filters for the 2012 processing year and stopped $1.3 billion in potentially fraudulent refunds as of April 19, 2012.[84]

The IRS first developed identity theft filters for use in processing year 2012.[85] Tax returns identified via the filter process are held until the IRS can verify the taxpayer's identity. In processing year 2012, there were 11 filters that identified approximately 325,000 returns and prevented the issuance of approximately $2.2 billion in fraudulent refunds. In processing year 2013, the number of filters increased to more than 80, and by May 30, 2013, the IRS had identified 151,000 returns and prevented the issuance of approximately $840 in fraudulent refunds.[86] For the 2014 processing year, the IRS has designed more identity theft screening filters.[87]

G. Identity Protection PIN

The IRS introduced the "Identity Protection PIN" (IP PIN) on the 2011 Form 1040, U.S. Individual Income Tax Return, (as well as on the simpler Forms 1040A and 1040EZ) and on the 2013 Form 1040NR, U.S. Nonresident Alien Income Tax Return (as well as on the simpler Form 1040NR-EZ and Form 1040-SS for certain residents of U.S. territories).

The IP PIN is a unique six-digit number that is assigned annually to victims of identity theft whose cases have been resolved. These individuals use the IP PIN when they file their federal tax return by entering it in the space provided next to the signature line. This identifies the return to the IRS as the return filed by the actual taxpayer. Tax returns can be filed electronically or on paper, but without the IP PIN, the IRS will not accept the return or issue a refund to the taxpayer. For the 2011 processing year, before Form 1040 included a specific area to enter the IP PIN, the IRS issued 53,700 IP PINs for taxpayers to use.[88] For the 2012 processing year, when the form included the

[81] For processing year 2012, the IRS received over 80% of returned electronically. http://www.irs.gov/uac/2012-Filing-Season-Statistics
[82] FS-2014-1, January 2014
[83] TIGTA, Ref. No. 2012-42-080, p. 4
[84] Id.
[85] TIGTA, Ref. No. 2013-40-122, p. 4
[86] Id.
[87] http://www.irs.gov/uac/Newsroom/IRS-Combats-Identity-Theft-and-Refund-Fraud-on-Many-Fronts-2014
[88] TIGTA, Ref. No. 2012-42-080, p. 5

entry space, 251,568 IP PINs were issued.[89] During this 2014 filing season, the IRS expects to provide more than 1.2 million victims with resolved cases with an IP PIN, up from more than 770,000 for the 2013 filing season.[90]

As part of its comprehensive identity theft strategy, the IRS has introduced a pilot project for the 2014 filing season. [91] It will provide an IP PIN to a limited number of taxpayers who filed their returns last year from Florida, Georgia and the District of Columbia, the three areas identified as having the highest per capita percentage of tax-related identity theft last year. The IP PINS provided through this pilot are in addition to the IP PINs that will be issued by the IRS for the 2014 filing season to known victims of identity theft. Even if the taxpayer has moved outside these 3 jurisdictions, the IP PIN may be offered for the 2014 filing season.

The IP PIN is available to taxpayers who filed in one of those three locations last year and who need, request, and successfully obtain an Electronic Filing PIN (e-file PIN) using the online application this year. People who need an e-file PIN include those who need to e-file a return but who do not have their Self-Select PIN (used by taxpayers to provide the IRS their prior year adjusted gross income) or AGI from their 2012 tax return in order to verify their identity to the IRS. Eligible taxpayers who request an e-file PIN using the online application while completing their federal tax return will be taken to a new IP PIN web application to validate their identity before receiving the IP PIN. This is done using a new web application where the taxpayer will be asked a series of questions only the taxpayer should be able to answer. If the taxpayer chooses not to participate in the pilot, he/she will file the tax return in the usual way and will receive any tax refund within the usual time frame.

Taxpayers who are offered the opportunity to obtain an IP PIN under the pilot program are encouraged, but are not required, to participate in the program. The IP PIN may be used on either electronic or paper returns. If the taxpayer chooses to participate and receive an IP PIN, the taxpayer must use it on the tax return. If the taxpayer files electronically and does not use the IP PIN, the tax return will not be processed. If the taxpayer files by paper, the return will be subjected to additional review to validate the taxpayer's identity. This review will delay the processing of the tax return and the issuance of any refund that may be due.

The knowledge gained from the pilot will help the IRS determine if or when the IP PIN can be offered to a larger number of taxpayers.

[89] Id.
[90] http://www.irs.gov/uac/Newsroom/IRS-Combats-Identity-Theft-and-Refund-Fraud-on-Many-Fronts-2014
[91] http://www.irs.gov/uac/Newsroom/2014-Identity-Protection-PIN-(IP-PIN)-Pilot

H. Applying Data Patterns to Prevent Future Identity Theft

In 2012, TIGTA reported that the IRS uses little of the data from the identity theft cases to identify trends, etc., that could be used to detect or prevent future refund fraud and recommended that the IRS adjust its processing to track and analyze trends and patterns.[92] For example, TIGTA's analysis of Tax Year 2010 returns with identity theft characteristics found that $8.1 million in potentially fraudulent tax refunds involved tax returns filed from one of five addresses.[93]

The IRS began initiatives in 2012 to better identify fraud cases. They include:

1. Establishing a team whose mission is to provide a formal mechanism for receiving, evaluating, and prioritizing new and emerging refund fraud referral issues, and developing and communicating IRS-wide solutions in real-time to protect revenue.

2. Implementing the Data Mining Inventory Reduction Effort to improve the IRS's ability to verify potentially fraudulent tax returns.

3. Establishing the Accelerated Screening Group to analyze tax returns to better identify potentially fraudulent tax returns. This includes better identification of fraud patterns, including those involving Schedule C income and household servant income.[94]

Although the IRS has improved the use of the filter process, TIGTA recommended in 2013 that the IRS continue to analyze characteristics of fraudulent tax returns resulting from identity theft to refine and expand filters.[95] In early 2014, the IRS indicated that it will continue to increase both the number and efficiency of the identity theft filters that are used to identify potentially fraudulent returns due to identity theft prior to the processing of the return and release of any refund.[96]

I. Real-Time Tax System

On December 8, 2011, the IRS Commissioner held the first public meeting to discuss the IRS's long-term initiative to move to a real-time tax system.[97] A real-time tax system would allow the IRS to verify many tax return elements at the time a tax return is filed and allow taxpayers to correct potential discrepancies before the IRS completes the processing of their tax return. Currently, it is not uncommon for a taxpayer to receive a notice 12 to 18 months after a tax return is filed. GAO issued a report in June 2013 that reviewed the 2010 and 2011 tax years. For tax year 2010, over a year passed on average before the IRS notified a taxpayer of discrepancies in matching third-party information and information on the taxpayer's return.[98] This can create both problems

[92] TIGTA Ref. No. 2012-40-050, p. 23
[93] TIGTA 2012-42-080, p. 9
[94] Id.
[95] TIGTA Ref. No. 2013-40-122, p. 17
[96] http://www.irs.gov/uac/Newsroom/IRS-Combats-Identity-Theft-and-Refund-Fraud-on-Many-Fronts-2014
[97] http://www.irs.gov/Tax-Professionals/December-8,-2011-Meeting
[98] GAO-13-515, *Tax Refunds: IRS Is Exploring Verification Improvements, but Needs to Better Manage Risks* (June 2013), p. 12. The average was 388 days.

and frustrations for the taxpayer and the IRS.[99] Of equal importance is that this type of tax system will allow the IRS to quickly identify fraudulent tax return filings based on false income reporting.[100] TIGTA has identified access to third-party income and withholding information at the time tax returns are processed as the single most important tool that the IRS could have to identify and prevent tax refund fraud.[101] Delayed access to third-party income and withholding information makes it difficult for the IRS to detect fraudulent tax refunds at the time tax returns are processed.[102] Third parties are not required to submit income and withholding documents to the IRS until March 31, yet taxpayers can begin filing tax returns in mid-January. For example, for tax year 2011, the IRS had issued 50 percent of the 2012 refunds by the end of February 2012, but it had received only 3 percent of information returns. By August, 2012, when the IRS completed its first match of information return data to tax returns, 92 percent of refunds had been issued.[103] Some information return providers routinely request filing extensions to provide the taxpayer with an opportunity to notify them of needed correction because of the penalties on filing forms with incorrect information.[104] However, legislative changes would be needed for any changes to the filing deadlines for information returns.[105]

An example of how a real-time system could work is provided with information on social security benefits. The IRS receives Form SSA-1099, Social Security Benefit Statement, in December. This form includes information on social security benefits and federal income tax withholding on those benefits. Use of Form SSA-1099 information would enable the IRS to ensure that all Social Security benefits and related withholding reported on tax returns are valid at the time the tax return is filed and before tax refunds are issued. In a 2012 report, TIGTA identified almost $232 million in potentially fraudulent tax refunds for which the false income and withholding claimed was for Social Security benefits.[106] At that time, the IRS had not established a process to match the information. The IRS began using Form SSA-1099 information during the 2012 filing season to identify tax returns with claims for withholding on Social Security benefits when there was no evidence of withholding on the Form SSA-1099. As a result, for the 2012 processing year, the IRS decreased the number of undetected tax returns based on fraudulent Social Security benefit income by 86 percent compared to the amount TIGTA has reported earlier.[107] The success continued in the 2013 processing year, when the IRS identified fraudulent 36,523 tax returns reporting $184 million in tax refunds.[108]

[99] http://www.irs.gov/pub/irs-utl/ir-2011-114.pdf
[100] TIGTA, Ref. No., 2012-42-080, p.5
[101] Id., p. 7, and TIGTA, Ref. No. 2013-40-122, p. 5
[102] In fact, Michael McKenney, Acting Deputy Inspector General for Audit, TIGTA, testified that while the IRS had made some progress in addressing identity theft, "there is a portion of the problem that cannot be fully addressed until the IRS receives income and withholding information before tax return processing. Access to third-party income and withholding information at the time tax returns are processed is the single most important tool the IRS could use to detect and prevent tax fraud-related identity theft resulting from the reporting of false income and withholding." Testimony of Michael McKenney, footnote 38, at p. 5
[103] GAO-13-515, p. 8
[104] GAO-13-515, p. 11
[105] TIGTA Ref. No. 2012-42-080, p 6
[106] TIGTA Ref. No.2012-42-080, p 13
[107] TIGTA Ref. No. 2013-40,122, p.6
[108] Id.

TIGTA has continued to report that the IRS still does not have timely access to all third-party income and withholding information that it could use to improve its fraud detection at the time returns are filed.[109] The IRS continues to address this problem, recognizing concerns from stakeholders that earlier reporting would increase data errors.[110]

TIGTA also has recommended, and the IRS has requested in previous budgets, expanded IRS access to the National Directory of New Hires (NDNH).[111] The NDNH is a database that contains information on all newly hired employees. The data include the six basic elements on Form W-4, Employee's Withholding Certificate, for newly hired employees: employee's name, address, and SSN, as well as the employer's name, address, and Federal Employer Identification Number. The NDNH also includes quarterly wage information for individual employees provided by State Workforce Agencies and Federal Agencies, and unemployment information for individuals who have received or applied for unemployment benefits. Currently the IRS can access the Directory to obtain information for tax returns claiming the Earned Income Tax Credit.[112] If legislation were enacted to grant the IRS the authority to receive extracts from the NDNH, this information, along with third-party income and withholding information that the IRS maintains for the prior year's tax filings, could allow the IRS to better identify individuals filing fraudulent tax returns. The IRS could design a process that uses prior year third-party wage and withholding reporting documents and NDNH data to determine if the reported wages and withholding on a tax return appear false.[113]

The Treasury Budget for Fiscal Year 2015 includes a proposal to require that all information returns be provided to the IRS by January 31, with the exception Form 1099-B, the Broker Statement.[114]

V. Conclusion

The IRS is faced with the dual, sometimes contradictory, goals of processing returns quickly to provide fast refunds while protecting taxpayers' identities and eliminating tax fraud. To achieve these goals, it uses many tools, including more sophisticated identity filters and grouping techniques as well as simple IP PINs that must be manually entered on a return. In recognition of these goals and challenges, the IRS has requested an increase in both funding and personnel to continue addressing identity theft, including an expansion of the specialized Criminal Investigation Identity Theft Clearinghouse that processes identity theft leads; and investment in information technology that will protect taxpayer information, help verify potentially fraudulent identity theft tax returns, and reduce erroneous payments.[115]

---

[109] Id., p 5
[110] Id., p. 7
[111] TIGTA Ref. No. 2012-42-080, pp. 7-8; Testimony of The Honorable J. Russell George (November 29, 2012), footnote 37, p. 3; Testimony of The Honorable J. Russell George Treasury Inspector General for Tax Administration, *Identity Theft and Tax Fraud*, before the Committee on Ways and Means, Subcommittees on Oversight and Social Security (May 8, 2012) , p. 4; Department of the Treasury, *General Explanations of the Administration's Fiscal Year 2014 Revenue Proposals*, p. 192
[112] TIGTA Ref. No. 2010-40-129, *Expanded Access to Wage and Withholding Information Can Improve Identification of Fraudulent Tax Returns* (September 30, 2010), p. 5
[113] TIGTA Ref. No. 2012-42-080, p 8
[114] Department of the Treasury, *General Explanations of the Administration's Fiscal Year 2015 Revenue Proposals*, p. 246
[115] U.S. Department of the Treasury, *Budget in Brief, Fiscal Year 2015*, p. 64