



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

March 25, 2008

Reference Number: 2008-40-086

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

March 25, 2008

MEMORANDUM FOR DEPUTY COMMISSIONER FOR OPERATIONS SUPPORT

FROM: *Michael R. Phillips*
Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft (Audit # 200740004)

This report presents the results of our review of the effectiveness of the Internal Revenue Service's (IRS) actions in assisting taxpayers victimized by identity theft with their current and future tax compliance issues and in pursuing action against individuals responsible for employment-related and tax fraud identity theft. This audit was conducted as part of our Fiscal Year 2007 Annual Audit Plan.

Impact on the Taxpayer

Identity theft is a growing national problem that increasingly affects tax administration. Although the IRS has increased its public outreach efforts, a proactive identity theft prevention approach is needed to effectively address employment-related and tax fraud identity theft so taxpayers will not continue to be victimized.

Synopsis

The IRS has not placed sufficient emphasis on employment-related and tax fraud identity theft strategies. Specifically, its prevention strategy does not include pursuing individuals using another person's identity, unless their cases directly relate to a substantive tax or conspiracy violation. IRS policy is that the actual crime of identity theft will only be investigated by the Criminal Investigation Division if it is committed in conjunction with other criminal offenses having a large tax effect.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

During Calendar Years 2005 and 2006, the Federal Trade Commission received 92,570 taxpayer complaints related to employment-related and tax fraud identity theft.¹ Due to the lack of IRS information related to identity theft, it is not clear whether the Criminal Investigation Division evaluated or investigated any of these complaints. According to the IRS, the Criminal Investigation Division does not use the Federal Trade Commission Identity Theft Clearinghouse data, and any identity theft prosecution recommendations would have been developed from other sources.

However, identity theft related to tax administration is rarely recommended for prosecution. In Fiscal Year 2005, only 45 cases recommended for prosecution included a charge of identity theft, and in Fiscal Year 2006, only 55 cases included this charge. Furthermore, actions taken in response to employment-related identity theft are not adequate to stop the unlawful use of the identity. Employers are notified of mismatches between names and Social Security Numbers. However, if both a taxpayer's name and Social Security Number are used by another person, employers are not notified and no further action is taken to stop the continued unlawful use of the identity.

IRS officials informed us that the IRS is unable to do more to stop continued use of someone's identity in employment-related identity theft cases. They stated that the IRS does not have sufficient enforcement resources to address most of these cases. Moreover, they believe that employment-related identity theft cases are not the responsibility of the IRS and that it would not be worthwhile to pursue employment-related identity theft cases for unreported tax liabilities because the taxes owed on most of these cases are not significant. Further, because of concerns with the reliability of the data, they do not use the Federal Trade Commission Identity Theft Clearinghouse to evaluate whether additional actions are needed to address complaints of tax-related identity theft. We are concerned that if the IRS takes no additional action to stop further use of another person's identity, then there is no deterrent to keep the problem from spreading.

The IRS has mainly focused on combating identity theft through public outreach. This included revising widely used documents to include information on identity theft, creating and maintaining an identity theft webpage on IRS.gov, and giving numerous identity theft presentations to the tax preparer community. Nonetheless, its current processes and procedures have been inadequate in reducing burden for taxpayers victimized by identity theft. For example:

- The Automated Underreporter function contacted taxpayers multiple times for the same compliance issues even though these taxpayers' cases were previously marked as closed for identity theft.

¹ The Treasury Inspector General for Tax Administration did not analyze the taxpayer complaints on the Federal Trade Commission Identity Theft Clearinghouse database. There may be some tax fraud complaints included in this number resulting from State income tax returns.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

- The Automated Underreporter system identity theft closing codes are not recognized by the Withholding Compliance function.

In addition, the IRS currently lacks the comprehensive data needed to determine the impact identity theft is having on tax administration.

Recommendations

We recommended that the Deputy Commissioner for Operations Support coordinate with the Deputy Commissioner for Services and Enforcement to develop and implement a strategy to address employment-related and tax fraud identity theft. This should include coordinating with other Federal agencies such as the Federal Trade Commission and Social Security Administration to evaluate and investigate identity theft allegations related to tax administration. The Deputy Commissioner for Operations Support should (1) coordinate with the Deputy Commissioner for Services and Enforcement to update the Automated Underreporter system to display prior year closing codes on the individual case screens and (2) create identity theft closing codes for multiple issue cases that will allow for individual underreporting issues to be closed as identity theft, and revise Withholding Compliance function case selection criteria to incorporate special handling of identity theft victims.

Response

IRS management generally agreed with all of our recommendations. However, management also discussed certain limitations in the actions that it will take. The IRS will continue to update its strategies to make its efforts more effective and efficient in the areas of identity theft awareness, prevention, detection and prosecution. IRS management is in the process of developing its vision for the future of the Privacy, Information Protection and Data Security office. Management stated that the Criminal Investigation Division is increasing the recommendations for prosecutions of identity theft cases under traditional statutes within the IRS' jurisdiction. However, management does not plan to more actively identify or stop individuals from committing employment-related identity theft or notify employers of the problem. Management stated that it is prevented by confidentiality and disclosure provisions in the Internal Revenue Code² from taking actions to stop continued use of another person's identity for employment and that it is broadly restricted from sharing taxpayer information with third parties. The IRS provided a copy of our report to the Office of the Assistant Secretary of the Treasury for Tax Policy to evaluate whether legislative remedy should be sought for this issue.

The IRS agreed that it should continue to improve its business processes and systems to reduce burden on identity theft victims. In January 2008, the IRS implemented the universal identity

² Internal Revenue Code Section 6103.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

theft indicator, which is placed on a taxpayer's account when the taxpayer self-identifies as an identity theft victim and provides the proper documentation to verify his or her identity. The use of this code standardizes the identification and tracking of identity theft accounts across all IRS functions and enables the IRS to centrally track incidents of identity theft, protect revenue threatened by identity fraud, and reduce taxpayer burden. Management stated that this universal code eliminates the need to update the Automated Underreporter system case screens and develop closing codes for multiple issue cases that will allow for individual underreporting issues to be closed as identity theft. The IRS will develop business rules for various programs, including the Criminal Investigation Division, Refund Crimes Unit, and the Automated Underreporter and Withholding Compliance functions, to apply unique treatments to cases when the universal identity theft indicator is present. The universal identity theft indicator and the closing codes will also be used as factors in the selection and prioritization of Automated Underreporter function cases in future years.

In its general discussion of the report, the IRS also provided additional statistics on its criminal prosecutions related to identity theft. Further, the IRS Privacy, Information Protection and Data Security office has recently engaged the Federal Trade Commission to collaborate in outreach activities and has received extracts of general information from the Identity Theft Clearinghouse to track trends and develop process improvement and outreach initiatives for victim assistance. The IRS also evaluated a sample of complaints in the Identity Theft Clearinghouse related to tax fraud. However, it found that the data generally did not provide enough details or personal information needed to support the initiation of an investigation. Management's complete response to the draft report is included as Appendix V.

Office of Audit Comment

We acknowledge the coordination now taking place between the Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and Enforcement and the efforts that the IRS has taken to reduce the burden on identity theft victims. We also believe that the effective use of the universal identity theft indicator should reduce the number of multiple contacts made with taxpayers.

We are concerned, however, that in its response, the IRS did not indicate the responsible officials or implementation dates for some of its actions. For example, the IRS needs to set specific action dates for implementing and testing new business rules and the processes needed to carry out those business rules for all affected programs. In addition, the IRS mentions implementing a 5-year strategy for its Privacy, Information Protection and Data Security office that will include identity theft issues. However, there is no mention of when this strategy will be implemented, what milestones will be established, and how its success will be measured.

The IRS provided statistics to show the increased number of tax returns identified by the Criminal Investigation Division's Fraud Detection Center involving refund crimes but did not



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

make it clear which portion of these refund crimes relate to identity theft. The IRS also provided statistics related to the number of victims associated with the identity theft prosecutions for Fiscal Years 2005 and 2006. However, the IRS did not provide this information during our audit or during the discussion of this report. As such, we cannot attest to the accuracy of these statistics. Given the number of cases reported to the Federal Trade Commission and the IRS, it is clear that only a small portion are investigated and recommended for prosecution.

We remained concerned about the lack of action on employment-related identity theft cases. The use of an incorrect Social Security Number for employment results in more government action to correct the problem than the use of someone else's complete identity (name and Social Security Number), even though the latter causes much more burden to the lawful taxpayer. We believe the IRS should take a more active role in working to stem this problem.

We commend the IRS effort to collaborate with the Federal Trade Commission in outreach activities and to use extracts of general information from the Identity Theft Clearinghouse to track trends and develop process improvements and outreach initiatives for victim assistance. However, we are concerned that the IRS has concluded that the Federal Trade Commission data are not useful in evaluating or investigating tax fraud or employment-related identity theft. Because the Identity Theft Clearinghouse is the sole national repository of consumer identity theft complaints, it should be an important source of data for the Criminal Investigation Division.

Please contact me at (202) 622-6510 if you have questions or Michael E. McKenney, Assistant Inspector General for Audit (Wage and Investment Income Programs), at (202) 622-5916.



*Outreach Has Improved, but More Action Is Needed to Effectively
Address Employment-Related and Tax Fraud Identity Theft*

Table of Contents

Background	Page 1
Results of Review	Page 5
Additional Actions Are Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft	Page 5
<u>Recommendation 1:</u>	Page 9
The Internal Revenue Service Has Improved Outreach Efforts and Documentation Standards	Page 10
Efforts Are Still Needed to Reduce Burden on Identity Theft Victims	Page 12
<u>Recommendation 2:</u>	Page 13
More Information Is Needed to Determine the Impact of Identity Theft on Tax Administration	Page 14
<u>Recommendation 3:</u>	Page 15
Appendices	
Appendix I – Detailed Objective, Scope, and Methodology	Page 17
Appendix II – Major Contributors to This Report	Page 19
Appendix III – Report Distribution List	Page 20
Appendix IV – Outcome Measures	Page 21
Appendix V – Management’s Response to the Draft Report	Page 23



*Outreach Has Improved, but More Action Is Needed to Effectively
Address Employment-Related and Tax Fraud Identity Theft*

Abbreviations

FTC	Federal Trade Commission
IRS	Internal Revenue Service
SSN	Social Security Number
U.S.C. §	United States Code Section



*Outreach Has Improved, but More Action Is Needed to Effectively
Address Employment-Related and Tax Fraud Identity Theft*

Background

Identity theft is a growing national problem that increasingly affects tax administration. Individuals who steal taxpayer identities affect the tax system in two ways.

- **Fraudulent Tax Returns** – An individual may use another person’s Social Security Number (SSN) to file a fraudulent tax return in order to steal a tax refund. Subsequently, the lawful taxpayer would have to prove his or her identity to correct his or her tax liability or refund.
- **Misreporting of Income** – An individual may use another person’s name and SSN to obtain employment. Because income earned is reported to the Internal Revenue Service (IRS) by the employer, it will appear to the IRS that the lawful taxpayer did not report all of his or her income on his or her tax return.

In October 1998, the Identity Theft and Assumption Deterrence Act¹ was enacted, which expanded the criminalization of fraud in connection with identification documents to cover the unlawful transfer and use of identity. The law defines identity theft as when someone “...knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.”

On May 10, 2006, the President’s Task Force on Identity Theft was established by Executive Order 13402.² This Task Force launched a new era in the fight against identity theft.

Recognizing the heavy financial and emotional toll that identity theft exacts from its victims, and the severe burden it places on the economy, President Bush called for a coordinated approach among government agencies to combat this crime by having a strategic plan which would aim to make the Federal Government’s efforts more effective and efficient in the areas of identity theft awareness, prevention, detection, and prosecution. The Task Force focused on several areas:

- **Law Enforcement** - The Task Force examined the tools law enforcement can use to prevent, investigate, and prosecute identity theft crimes; recover the proceeds of these crimes; and ensure just and effective punishment of identity thieves.
- **Education** - The Task Force surveyed current education efforts by government agencies and the private sector on how individuals and corporate citizens can protect personal data.

¹ Pub. L. No. 105-318, 112 Stat. 3007 (codified in part of 18 U.S.C. §1028).

² Source of information about the President’s Task Force can be found at idtheft.gov.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

- **Government Safeguards** - Because government must help reduce, rather than exacerbate, incidents of identity theft, the Task Force worked with many federal agencies to determine how the government can increase safeguards to better secure the personal data that it and private businesses hold.

In April 2007, the President's Identity Theft Task Force³ strategic report recommended a plan designed to strengthen the efforts of Federal, State, and local law enforcement officers; to educate consumers and businesses on deterring, detecting, and defending against identity theft; to assist law enforcement officers in apprehending and prosecuting identity thieves; and to increase the safeguards used by Federal agencies and the private sector with respect to the personal data they hold.

The President's Identity Theft Task Force strategic report noted four major strategies for preventing and deterring identity theft were (1) establishing a data breach policy for the public sector, (2) improving data security in the public sector, (3) decreasing the use of SSNs by the public sector, and (4) publication for a routine use for disclosure of information following a data breach.

The Federal Trade Commission (FTC) is the primary Federal agency responsible for receiving identity theft complaints⁴ and maintains the Identity Theft Clearinghouse.⁵ According to the FTC, 56,125 (22 percent) of 258,427 of all reported identity theft complaints in Calendar Year 2007 resulted from either the filing of a fraudulent tax return or the misuse of someone's identity to obtain employment. From Calendar Years 2002 to 2007, the number of fraudulent tax returns filed as a result of identity theft increased 579 percent. In addition, the number of complaints resulting from employment-related identity theft more than doubled during the same time period. Figure 1 provides details on the number of identity theft complaints related to tax administration received by the FTC between Calendar Years 2002 and 2007.

³ The President's Identity Theft Task Force, *Combating Identity Theft A Strategic Plan*, April 2007.

⁴ Taxpayers may file identity theft complaints by filling out a form on the FTC's web site, calling the FTC Identity Theft Hotline, or writing a letter to the Identity Theft Clearinghouse.

⁵ The Identity Theft Clearinghouse is the sole national repository of consumer complaints about identity theft.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

Figure 1: Identity Theft Complaints Received by the FTC⁶

Identity Theft Complaints	Calendar Year						Percentage Increase From 2002-2007
	2002	2003	2004	2005	2006	2007	
Total	161,819	214,905	246,882	255,627	246,124	258,427	60%
Fraudulent Tax Returns	3,061	8,041	9,563	12,165	15,442	20,782	579%
Percent of Total	1.9%	3.7%	3.9%	4.8%	6.3%	8.0%	
Employment-Related	15,089	24,084	31,379	31,094	33,869	35,343	134%
Percent of Total	9.3%	11.2%	12.7%	12.2%	13.8%	13.7%	

Source: Federal Trade Commission – Identity Theft Clearinghouse.

In July 2005, the Treasury Inspector General for Tax Administration reported⁷ that the IRS lacked a corporate strategy to adequately address identity theft issues. The IRS agreed to develop (1) updated agency-wide communication tools to be used to educate and assist taxpayers with information about identity theft, (2) agency-wide standards to ensure the information taxpayers were asked to provide to substantiate identity theft claims is consistent throughout the IRS, and (3) specific closing codes for cases involving identity theft that could allow the IRS to track and monitor the effect of identity theft on tax administration.

In October 2005, the IRS established the Identity Theft Program Office in the Wage and Investment Division to develop centralized policy and procedural guidance. The Program Office was responsible for implementing the IRS Enterprise Identity Theft Strategy that is comprised of the following three components:

- **Prevention** – The IRS Criminal Investigation Division, Refund Crimes Unit, works to identify fraudulent tax returns filed by criminals using another person’s tax information in order to steal a tax refund.
- **Outreach** – The IRS alerts the public about possible identity theft scams through news articles and revised its most widely used tax documents to include identity theft information.
- **Victim Assistance** – The IRS revised its internal procedures and worked with the Social Security Administration to reduce the time needed to resolve “scrambled” SSNs. When

⁶ The Treasury Inspector General for Tax Administration did not analyze the taxpayer complaints on the FTC Identity Theft Clearinghouse database. There may be some tax fraud complaints included in these numbers resulting from State income tax returns.

⁷ *A Corporate Strategy Is Key to Addressing the Growing Challenge of Identity Theft* (Reference Number 2005-40-106, dated July 2005).



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

two tax returns are filed under the same SSN and the IRS cannot determine the true owner of the SSN, the “scrambled” SSN is sent to the Social Security Administration for verification. In the interim months (which previously took up to 2 years), the affected taxpayers would not be entitled to credits and/or refunds related to their SSN. The IRS is also updating its processes and notices to provide help to taxpayers whose names and SSNs were used by an identity thief for employment purposes.

The Identity Theft Program Office was also responsible for conducting detailed Identity Theft Risk Assessments of 36 IRS processes to identify internal areas that would be susceptible to identity theft. As a result of these risk assessments, 134 strategies were developed to address identified risks of which the IRS plans to expedite 3 of these strategies (i.e., Incident Response, Incident Tracking, and Enterprise-wide Encryption) for immediate implementation.

According to the IRS, the Identity Theft Program was transferred from the Wage and Investment Division to the IRS Mission Assurance and Security Services function in September 2006. In May 2007, IRS officials informed us that the new program office was not yet fully staffed. They also stated that the personnel responsible for the Identity Theft Program Office in the Mission Assurance and Security Services function had been busy working on Congressional testimony and implementing an incident response database to track inadvertently disclosed and/or stolen SSNs from the IRS or its systems. In July 2007, responsibility for the Identity Theft Program was assigned to the Deputy Commissioner for Operations Support. According to the IRS, “. . . reporting directly to a Deputy Commissioner will provide this program the ability to reach across all IRS organizations to ensure that proper attention and discipline is given . . .” to this important issue.

The focus of our review was on the effect of identity theft on taxpayers and tax administration. Accordingly, we focused on the oversight provided by the Wage and Investment Division Identity Theft Program Office and the handling of identity theft issues in the Automated Substitute for Return, Automated Underreporter, and Withholding Compliance functions. This review was performed in the Automated Substitute for Return and Automated Underreporter functions in the Small Business/Self-Employed Division in New Carrollton, Maryland, and the Identity Theft Program Office, Automated Substitute for Return, Automated Underreporter, and Withholding Compliance functions in the Wage and Investment Division in Atlanta, Georgia, during the period December 2006 through July 2007. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

Results of Review

Additional Actions Are Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

Tax fraud identity theft is rarely prosecuted

The IRS Enterprise Identity Theft Strategy for prevention does not include pursuing individuals using another person's identity, unless their cases directly relate to tax fraud. Employment-related fraud cases worked by the Criminal Investigation Division address employment tax issues but do not address the illegal use of SSNs for employment. The actual crime of identity theft is investigated by the Criminal Investigation Division only if it was committed in conjunction with other criminal offenses that have a large tax effect.

The Criminal Investigation Division section of the Internal Revenue Manual⁸ states that identity theft can be investigated in conjunction with money laundering and refund fraud. However, it also states that identity theft should be pursued only if it enhances the overall investigative strategy. An identity theft violation is not intended to stand alone, but it "must have a direct link to the substantive tax or the related conspiracy violation that is the focus of the criminal investigation." Rarely would it occur that an "identity theft is charged without a companion substantive tax or related conspiracy violation."

Figure 2 shows for Fiscal Years 2005 and 2006 the total number of prosecution recommendations made by the IRS Criminal Investigation Division compared to the total number of prosecution recommendations made in conjunction with identity theft. The majority of the cases in which the Criminal Investigation Division recommends prosecution for identity theft came from the Questionable Refund Program.⁹

⁸ The Internal Revenue Manual is a manual containing the IRS' internal guidelines.

⁹ The Questionable Refund Program was designed to identify fraudulent tax returns, to stop the payment of fraudulent refunds, and to refer identified fraudulent refund schemes to Criminal Investigation Division field offices.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

Figure 2: Total Prosecution Recommendations in Comparison With Identity Theft-Related Prosecution Recommendations

Prosecution Recommendations	Fiscal Year 2005	Fiscal Year 2006
Total Prosecution Recommendations Made by IRS Criminal Investigation Division	2,859	2,720
Prosecution Recommendations Made by IRS Criminal Investigation Division That Include Identity Theft	45	55
Percentage	1.6%	2.0%

Source: Criminal Investigation Management Information System.

In addition, the Criminal Investigation Division works fraud referrals that come in from various IRS functions, as well as outside interests (e.g., the Department of Justice, taxpayers). IRS management from the Automated Underreporter, Automated Substitute for Return, and Withholding Compliance functions stated that identity theft cases are referred to the Criminal Investigation Division. According to the IRS, the Criminal Investigation Division received only 625 fraud referrals in Fiscal Year 2005 and 603 fraud referrals in Fiscal Year 2006. These referrals may include, but are not limited to, identity theft cases. However, because there is no unique coding for identity theft referrals, there is no way to determine if any of these fraud referral cases were related to identity theft.

More needs to be done to address employment-related identity theft

The use of another person’s SSN to obtain employment is often done in conjunction with a name different from Social Security Administration records. This is known as an SSN/name mismatch. In these instances, the IRS and the Social Security Administration do not associate the income and benefits with the lawful taxpayer. The number of Wage and Tax Statements (Form W-2) with SSN/name mismatches is substantial. The Social Security Administration maintains an Earnings Suspense File for wage information reported on the Forms W-2 where the SSN and name do not match. This file contains approximately 264 million mismatched Forms W-2 related to \$586 billion in wages through the end of Calendar Year 2004. In some cases, the Social Security Administration has tried to correct these mismatches by notifying employers of the errors on the Forms W-2 through a “no match” letter. Employers who receive these letters are requested to take steps to correct the mismatch issue for each SSN that failed verification with Social Security Administration records. If the employer does not make an effort to correct the Forms W-2, the IRS can assess a penalty. Both the



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

Treasury Inspector General for Tax Administration and the Government Accountability Office have issued reports that address the tax problems related to SSN/name mismatches.¹⁰

While SSN/name mismatches are a significant problem for the IRS and the Social Security Administration, the more serious problem develops for the lawful taxpayer when both their name and SSN are used by someone else to gain employment. No action is taken to stop someone from continuing to commit employment-related identity theft using another person's SSN and name. The IRS does not actively try to identify or stop an individual from committing identity theft. Moreover, the IRS does not notify the employer of the problem of their employee using someone else's identity. Because the IRS and the Social Security Administration will assume the information on the Forms W-2 is accurate, the earnings resulting from the identity theft will be attributed to the lawful taxpayers for determining both Social Security benefits and tax liabilities. The IRS generally does not pursue the taxes that may be due on income earned using a stolen identity.

For example, wages earned by individuals using another person's identity would not be reported on the lawful taxpayer's tax return. Because the name and SSN on the Forms W-2 match IRS records, the IRS would assume the unreported wages belonged to the taxpayer. As a result, the IRS Automated Underreporter function¹¹ would send a notice to the taxpayer for the underreporting of income. If the taxpayer provides adequate documentation to prove identity theft, the IRS will remove the income and tax liability from the taxpayer's account and close the case. For Tax Years 2003 and 2004, more than 27,000 lawful taxpayers had to resolve underreporter problems with the IRS Automated Underreporter function as a result of employment-related identity theft. For Tax Year 2004 alone, approximately \$550 million in wages was reported for identity theft victims contacted by the Automated Underreporter function. We estimate approximately \$268 million (49 percent) of these total wages resulted from identity theft.¹²

During discussions with IRS management, they informed us that the IRS is unable to do more to stop continued use of someone's identity in employment-related identity theft cases. They provided the following reasons:

- Notifying employers that their employee is using another person's identity is not permissible because it would be an unlawful disclosure of tax information.

¹⁰ *Mismatched Names and Identification Numbers on Information Documents Could Undermine Strategies for Reducing the Tax Gap* (Reference Number 2007-30-159, dated August 31, 2007) and *TAX ADMINISTRATION: IRS Needs to Consider Options for Revising Regulations to Increase the Accuracy of Social Security Numbers on Wage Statements* (GAO-04-712, dated August 2004).

¹¹ The Automated Underreporter function issues notices informing taxpayers of discrepancies found when matching information return data received from third parties with income and deductions reported on tax returns.

¹² Since multiple individuals committing identity theft are using the same taxpayer name and SSN, we were not able to estimate the tax effect resulting from the individual identity thefts.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

- The IRS does not have sufficient enforcement resources to address most of these cases.
- The responsibility for employment-related identity theft cases is not within the jurisdiction of the IRS. Further, due to disclosure rules, IRS officials expressed concerns about sharing information on these cases with other agencies.
- It would not be worthwhile to pursue employment-related identity theft cases for unreported tax liabilities because, according to IRS officials, the taxes owed on most of these cases are not significant.
- The FTC Identity Theft Clearinghouse is not reliable; therefore, the Criminal Investigation Division does not use the FTC database to evaluate whether additional actions are needed to address complaints of tax-related identity theft.

While the IRS must often make resource allocation decisions based upon the tax effect of those resources, areas that affect taxpayer rights must also be addressed. In tax fraud and employment-related identity theft cases, the IRS is usually the first agency to become aware of the problem and has the information needed to address the identity theft. If the IRS takes no additional action to stop further use of another person's identity, then there is no deterrent to keep the problem from spreading.

The President's Task Force on Identity Theft recommends that law enforcement agencies continue to conduct enforcement initiatives that focus exclusively or primarily on identity theft. However, the Task Force recognized that there are limitations on the number of cases that can be prosecuted in the courts. Whether or not substantial increases in prosecutions are achievable, investigation and authentication of identities in the instances of reported identity theft would be a significant step in stopping the continued use of another person's identity, especially in employment-related cases.

Use of another person's identity for employment results in the misreporting of income which affects income tax and social security tax as well as other employment taxes. Agencies with jurisdiction over these matters include the IRS and the Social Security Administration. Consequently, coordination between these agencies is important to ensure that Federal records related to income earned by a taxpayer are correct and to ensure appropriate law enforcement. Federal law¹³ allows the Social Security Administration to pursue criminal penalties for an individual who fraudulently obtains, uses, or represents a SSN to be theirs. There are a number of exceptions in the Internal Revenue Code that allow disclosure of taxpayer information in order to investigate illegal activity. If the IRS believes these exceptions are not adequate for the purposes of combating identity theft, IRS management should seek legislative remedy through the Office of the Assistant Secretary of the Treasury for Tax Policy.

¹³ 42 U.S.C. §408 provides for criminal penalties for an individual who fraudulently buys, sells, or possesses a Social Security card with intent to sell or alter and where it is also a violation of this statute to disclose, use, or compels the disclosure of the SSN of any person in violation of the laws of the United States.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

In regard to IRS management's concerns about the reliability of data in the FTC Identity Theft Clearinghouse, because the IRS has not received or evaluated this data, it is not clear how IRS management concluded the data were unreliable. We did not audit the information in the database. However, we traced a limited number of underreporter cases that were related to identity theft back to the Identity Theft Clearinghouse, and the data on these cases appeared to be reported accurately. The complaints in the database would need to be further evaluated and investigated by the IRS to determine whether the complaints can be substantiated. Such an evaluation could help the IRS in developing a strategy to stem the increase in tax fraud and employment-related cases.

Recommendation

Recommendation 1: The Deputy Commissioner for Operations Support should coordinate with the Deputy Commissioner for Services and Enforcement to develop and implement a strategy to address employment-related and tax fraud identity theft. This should include coordinating with other Federal agencies such as the FTC and the Social Security Administration to evaluate and investigate identity theft allegations related to tax administration.

Management's Response: IRS management agreed that aggressive pursuit of identity theft criminals is a deterrent to identity theft. The IRS is developing a 5-year strategy for the Privacy, Information Protection and Data Security office, and will continue to improve strategies focused on tax fraud identity theft. The Criminal Investigation Division is increasing the recommendations for prosecutions of identity theft cases under traditional statutes within the IRS' jurisdiction as directed by the Department of Justice Tax Division.

The President's Identity Theft Task Force identified the Social Security Administration Office of Inspector General and the Department of Homeland Security as lead agencies to address identity theft. The IRS will work with these agencies to implement the Task Force recommendations.

IRS management does not plan to more actively try to identify or stop individuals from committing employment-related identity theft and notify employers of their employees using someone else's identity. It stated that under Internal Revenue Code Section 6103, the IRS is broadly restricted from sharing taxpayer information with third parties. The IRS provided a copy of this report to the Office of the Assistant Secretary of the Treasury for Tax Policy to evaluate whether legislative remedy should be sought.

Recently, the IRS obtained data from the FTC Identity Theft Clearinghouse and evaluated a sample of the Fraudulent Tax Return Filed complaints. The Criminal Investigation Division concluded that the data generally did not provide enough details or personal information to support the initiation of an investigation and, according to the FTC, the information has not been verified or authenticated by the FTC. Consequently,



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

the Criminal Investigation Division generally relies on alternative data sources to support specific cases recommended for criminal tax prosecutions.

Office of Audit Comment: We acknowledge the coordination now taking place between the Deputy Commissioner for Operations Support and the Deputy Commissioner for Services and Enforcement and the efforts that the IRS has taken to reduce the burden on identity theft victims.

Nonetheless, we remain concerned about the lack of action on employment-related identity theft cases. The use of an incorrect SSN for employment results in more government action to correct the problem than the use of someone else's complete identity (name and SSN) even though the latter causes much more burden to the lawful taxpayer. We believe that the IRS, in coordination with the Social Security Administration, should take a more active role in working to stem this problem.

We commend the IRS' effort to collaborate with the FTC in outreach activities and to use extracts of general information in the Identity Theft Clearinghouse to track trends and develop process improvements and outreach initiatives for victim assistance. However, we are concerned that the IRS has concluded that the FTC data are not useful in evaluating or investigating tax fraud or employment-related identity theft. The Identity Theft Clearinghouse is the sole national repository of consumer identity theft complaints. It should be an important source of data for the Criminal Investigation Division.

The Internal Revenue Service Has Improved Outreach Efforts and Documentation Standards

Since our July 2005 report, the Identity Theft Program Office has focused mostly on its Enterprise Identity Theft Strategy for public outreach. To date, the Program Office has been responsible for:

- Revising widely used documents, such as the Form 1040¹⁴ Instruction Booklet and *Your Federal Income Tax* (Publication 17), to include information on identity theft.
- Creating and maintaining an identity theft webpage on IRS.gov that provides taxpayers with updated information regarding identity theft issues and also provides links to other Federal Government agencies (e.g., the Social Security Administration and the FTC) that may be of assistance to victims of identity theft.
- Creating the DVD *Identity Theft Outsmarting the Crooks* and the publication *Identity Theft Prevention and Victim Assistance* that provides valuable information to taxpayers concerning identity theft issues.

¹⁴ U.S. Individual Income Tax Return.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

- Issuing public service announcements stating that the IRS does not communicate with taxpayers via email in an effort to reduce the number of identity thefts resulting from “phishing.”¹⁵
- Partnering with the Treasury Inspector General for Tax Administration’s Office of Investigation to create the “Phishing In-Box,” which is an email address to which taxpayers can send suspicious emails they believe may be part of a “phishing” scam.
- Giving numerous identity theft presentations to the tax preparer community at various events, such as the IRS tax forums.

The Identity Theft Program Office was also involved in establishing the Identity Theft Policy Statement which states that the IRS will take the necessary steps to provide assistance to identity theft victims and recognize the need for timely resolution of taxpayer account issues caused by identity theft.

Documentation standards have been improved

In Fiscal Year 2006, after conducting an extensive Identity Theft Risk Assessment, the IRS found that its inconsistent documentation standards, which we reported on in our July 2005 report, might have resulted in unnecessary burden for taxpayers attempting to resolve adverse tax situations caused by identity theft. The IRS acknowledged that under prior procedures, taxpayers were required to present different sets of documentation each time they dealt with different IRS functional groups. As a result, in June 2007, the IRS issued a memorandum to its employees that established a consistent agency-wide standard when requesting written documentation from taxpayers to resolve their identity theft cases. Specifically, these new documentation requirements consist of two parts.

- Authentication of Identity – a copy of a valid United States Federal or State government issued form of identification (e.g., driver’s license, State identification card, social security card, passport, etc.).
- Evidence of Identity Theft – a copy of a police report or an Identity Theft Affidavit filed with the FTC.

¹⁵ Phishing is a scam in which Internet fraudsters send email messages to trick unsuspecting victims into revealing personal and financial information that can be used to steal the victims’ identity.



Efforts Are Still Needed to Reduce Burden on Identity Theft Victims

The IRS Enterprise Identity Theft Strategy for victim assistance has been insufficient in reducing burden for taxpayers victimized by identity theft. In general, it can be a very frustrating and time consuming process for taxpayers who are identity theft victims to resolve their issues with the IRS.

Some identity theft victims were unnecessarily contacted multiple times by various functions

The IRS Automated Underreporter function uses unique closing codes on its Automated Underreporter system to identify cases closed as identity theft. However, adding these closing codes was not sufficient to stop multiple contacts with the taxpayers.

As of November 2006, the IRS closed 12,617 Tax Year 2003 cases and 14,729 Tax Year 2004 cases on its Automated Underreporter system as a result of identity theft. Our analysis of these Tax Year 2003 and 2004 cases found that 449 (3.6 percent of the Tax Year 2003 identity theft cases) were selected and closed as identity theft for the same underreported issue in both years. We found an additional 184 cases that were similarly closed as identity theft in Tax Year 2005. In each of these cases, taxpayers were contacted even though identity theft closing codes were already posted on the Automated Underreporter system for a prior year underreporting issue.

Figure 3 provides details on the 633 identity theft cases selected and closed for the same underreported issue in 2 or more years by the Automated Underreporter function.

Figure 3: Taxpayers Contacted by the Automated Underreporter Function for the Same Issue in 2 or More Years Due to Identity Theft

Business Operating Division	Number of Taxpayers
Small Business/Self-Employed Division	48
Wage and Investment Division	585
Total	633

Source: Individual Master File¹⁶ and Automated Underreporter system extract provided by the IRS.

The Automated Underreporter function is currently finishing work on its inventory of Tax Year 2005 cases. Our analysis of the Individual Master File for these cases identified an additional 607 Tax Year 2005 cases open as of March 2007 where the taxpayers were contacted for the same underreported issue that was previously closed as identity theft in one or more of the prior years. Because underreported income resulting from employment-related identity theft tends to

¹⁶ The IRS database that maintains transactions or records of individual tax accounts.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

be a multi-year issue, we believe these Tax Year 2005 cases will be closed as identity theft as well. In addition, we identified another 34 Tax Year 2005 cases that were closed as “no change” for the same underreported issues that had been previously closed as identity theft in a prior year.

Once the Automated Underreporter cases were selected, examiners manually screened them to verify that income was underreported. Currently, the individual case screens on the Automated Underreporter system do not show prior year closing codes. Without performing additional research on the Individual Master File, examiners would not know if a taxpayer’s case was closed by the Automated Underreporter function as identity theft in a prior year. Consequently, 1,274 identity theft victims were unnecessarily contacted multiple times by the Automated Underreporter function. We estimate for Tax Year 2004, the IRS was unable to make approximately \$440,020 in potential tax assessments¹⁷ as a result of working these unproductive cases and not working more productive Automated Underreporter function cases. If the IRS does not correct this problem, we estimate that over 5 years \$2.2 million in tax assessments may be lost.

In addition, we identified another 55 Tax Year 2003 identity theft cases closed by the Automated Underreporter function in which the taxpayers were subsequently contacted by the Withholding Compliance function for underwithholding issues in Tax Year 2004. This occurred because the Withholding Compliance function case creation criterion does not consider prior year Automated Underreporter function identity theft closing codes. In responding to our results, the Withholding Compliance function agreed that other IRS functions’ identity theft codes should be considered.

Recommendation

Recommendation 2: The Deputy Commissioner for Operations Support should coordinate with the Deputy Commissioner for Services and Enforcement to:

- Update the individual case screens on the Automated Underreporter system to display prior year closing codes.
- Ensure revision of the Withholding Compliance function case selection criteria to incorporate special handling of identity theft victims.

Management’s Response: IRS management agreed that it should continue to seek opportunities to improve business processes and technology systems to further reduce taxpayer burden and eliminate multiple contacts of identity theft victims. The IRS is currently developing a 5-year strategy for its Privacy, Information Protection and Data

¹⁷ The \$440,020 was calculated by multiplying the 449 identity theft taxpayers that were contacted by the Automated Underreporter function for the same compliance issues in Tax Years 2003 and 2004 by the average Automated Underreporter function assessment rate for Tax Year 2004, which was \$980.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

Security office that will include identity theft issues. In January 2008, the IRS implemented the universal identity theft indicator, which is placed on a taxpayer's account when the taxpayer self-identifies as an identity theft victim and provides the proper documentation to verify his or her identity. The use of this code standardizes the identification and tracking of identity theft accounts across multiple tax modules in all IRS functions. This solution supersedes the need to update the individual Automated Underreporter system case screens. In addition, the IRS will develop business rules for various programs, including the Criminal Investigation Division, Refund Crimes Unit, and the Automated Underreporter and Withholding Compliance functions, to apply unique treatments to cases when the universal identity theft indicator is present.

Office of Audit Comment: We acknowledge that the effective use of the new universal identity theft indicator should reduce the number of multiple contacts with taxpayers in both the Automated Underreporter and Withholding Compliance functions. However, the IRS needs to set specific action dates for implementing and testing new business rules and the processes needed to carry out those business rules for all affected programs. In addition, the IRS mentions implementing a 5-year strategy for its Privacy, Information Protection and Data Security office that will include identity theft issues. However, there is no mention of when this strategy will be implemented, what milestones will be established, and how its success will be measured.

More Information Is Needed to Determine the Impact of Identity Theft on Tax Administration

The IRS currently lacks the comprehensive data needed to determine the impact identity theft has on tax administration. However, the IRS is in the process of establishing a universal identity theft indicator on the Individual Master File. The purpose of this indicator will be to centrally track incidents of identity theft, protect Department of the Treasury revenue threatened by identity fraud, and reduce taxpayer burden related to identity theft. The IRS stated the universal identity theft indicator will be online in Calendar Year 2008.

Since Fiscal Year 2005, only the Automated Underreporter function has been able to identify taxpayer cases closed as identity theft. The Automated Underreporter function uses program-specific closing codes to mark incidents of identity theft on its Automated Underreporter system. The program-specific closing codes will be used to generate the universal identity theft indicator on the Individual Master File for these Automated Underreporter function cases. However, the Automated Underreporter function does not consistently use these codes on multiple issue identity theft closures. Automated Underreporter function personnel use identity theft closing codes only on cases that result in a no change in the tax liability. This occurs because Automated Underreporter function personnel do not have a choice of closing codes that allow for multiple issue case closures involving identity theft.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

For example, if a taxpayer was selected for a combination of underreported wages and interest but proves the underreported wages were a result of identity theft, the IRS would still assess additional tax on the underreported interest income. Because a tax assessment was made on the underreported interest income, the Automated Underreporter function would not code this case as identity theft on the Automated Underreporter system. As a result, taxpayers with some underreported wage issues resulting from identity theft may be unnecessarily burdened by future contacts from the IRS. In addition, the number of identity theft closures made by the Automated Underreporter function could be significantly understated as a result of single issues on multiple issue case closures not being coded individually as identity theft.

To put this into perspective, the Automated Underreporter function selected almost 4.5 million cases to review from Tax Year 2005. According to the IRS, most of the selection categories could include multiple issue cases. Because the Automated Underreporter function does not have an identity theft closing code for multiple issue cases, none of the multiple issue cases would be coded as identity theft if there was a tax assessment made on one of the underreported issues.

To date, the IRS' actions related to identity theft have been mostly reactive in assisting taxpayers when they contact the IRS as a result of a notice and/or other type of enforcement action. In many instances, this is the first time the taxpayer learns that he or she is a victim of identity theft. Due to the lack of identity theft information available, the IRS is unable to identify specific trends, measure the success of the Enterprise Identity Theft Strategy, and take proactive steps to reduce the burden on impacted taxpayers.

Recommendation

Recommendation 3: The Deputy Commissioner for Operations Support should coordinate with the Deputy Commissioner for Services and Enforcement to establish closing codes for multiple issue cases on the Automated Underreporter system that will allow for individual underreporting issues to be closed as identity theft.

Management's Response: IRS management agreed that additional information about identity theft cases is needed to determine the impact of identity theft on tax administration. In January 2008, the IRS implemented the universal identity theft indicator to centrally track incidents of identity theft, protect revenue threatened by identity fraud, and reduce taxpayer burden related to identity theft. The universal identity theft indicator supersedes the need for the Automated Underreporter Program to develop a new system to report multiple closing codes. The universal identity theft indicator and the closing codes will also be used as factors in the selection and prioritization of Automated Underreporter function cases in future years.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

Office of Audit Comment: New Automated Underreporter Program procedures¹⁸ provide for manual input of the universal identity theft indicator in multiple issue cases when one of the issues involves identity theft. If this process operates as intended, it should be sufficient to address our recommendation.

¹⁸ Internal Revenue Manual Procedural Update No. C IMF 080099 dated January 28, 2008, and Internal Revenue Manual Procedural Update No. C IMF 080108 dated January 30, 2008.



Appendix I

Detailed Objective, Scope, and Methodology

Our overall audit objective was to evaluate the effectiveness of the IRS' actions in assisting taxpayers victimized by identity theft with their current and future tax compliance issues and in pursuing action against individuals responsible for employment-related and tax fraud identity theft. Unless otherwise noted, our limited tests of the reliability of data obtained from IRS systems did not identify any errors. We tested the reliability of the data by scanning the data received for blank, incomplete, illogical, or improper data. In addition, we traced a judgmental sample for each data set to the source IRS files to ensure accuracy. We did not perform any testing of internal controls over the systems that were the sources of our data. To accomplish the objective, we:

- I. Determined if the IRS effectively addresses the current and future tax compliance issues of taxpayers identified as victims of identity theft by interviewing and obtaining documentation from the Identity Theft Program Office and the Automated Substitute for Return, Automated Underreporter, and Withholding Compliance functions about how the IRS processes identity theft cases.

We researched the FTC web site and reviewed documentation to determine the information captured by the FTC Identity Theft Clearinghouse¹ and the Identity Theft Affidavit.

We researched the Social Security Administration web site and reviewed documentation to determine its guidelines for SSNs that do not match.

- II. Identified the number of taxpayers who were contacted in multiple years by the Automated Underreporter function concerning the same identity theft issue. We analyzed the Tax Years 2003 and 2004 Automated Underreporter function identity theft cases and identified taxpayers who were contacted for the same identity theft issue for both years. In addition, we queried the Tax Year 2005 Individual Master File² and an IRS-provided Automated Underreporter system extract and identified previously coded identity theft taxpayers selected again for the same issue.
- III. Identified the number of identity theft victims who were contacted by the Withholding Compliance function during Fiscal Year 2006 after they had substantiated identity theft with the Automated Underreported function for Tax Years 2003 and/or 2004 for wage issues.

¹ The Identity Theft Clearinghouse is the sole national repository of consumer complaints about identity theft.

² The IRS database that maintains transactions or records of individual tax accounts.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

- IV. Determined what actions the IRS takes to identify individuals using another person's identity by interviewing and obtaining documentation from the Identity Theft Program Office and the Automated Substitute for Return, Automated Underreporter, and Withholding Compliance functions.
- V. Determined if the IRS effectively investigates identity theft cases for criminal prosecution by interviewing Criminal Investigation Division management to determine the IRS' jurisdiction for investigating identity theft cases for criminal prosecution and obtained statistics of identity theft cases.
- VI. Determined if the IRS effectively monitors and measures the success of the Identity Theft Program by interviewing and obtaining documentation from the Identity Theft Program Office and Automated Substitute for Return, Automated Underreporter, and Withholding Compliance functions.



*Outreach Has Improved, but More Action Is Needed to Effectively
Address Employment-Related and Tax Fraud Identity Theft*

Appendix II

Major Contributors to This Report

Michael E. McKenney, Assistant Inspector General for Audit (Wage and Investment Income Programs)
Mary V. Baker, Director
Marybeth Schumann, Director
Bryce Kisler, Director (Acting)
Alan Lund, Audit Manager (Acting)
Julia Tai, Lead Auditor
Sharon Summers, Senior Auditor
Jean Kao, Auditor



*Outreach Has Improved, but More Action Is Needed to Effectively
Address Employment-Related and Tax Fraud Identity Theft*

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Acting Chief of Staff C
Deputy Commissioner for Services and Enforcement SE
Commissioner, Small Business/Self-Employed Division SE:S
Commissioner, Wage and Investment Division SE:W
Chief Counsel CC
Chief, Privacy, Information Protection and Data Security OS:PIPDS
Director, Campus Filing and Payment Compliance, Small Business/Self-Employed Division
SE:S:CCS
Director, Campus Reporting Compliance, Small Business/Self-Employed Division SE:S:CCS
Director, Compliance, Wage and Investment Division SE:W:CP
Director, Strategy and Finance, Wage and Investment Division SE:W:S
Director, Filing and Payment Compliance, Wage and Investment Division SE:W:CP:FPC
Director, Reporting Compliance, Wage and Investment Division SE:W:CP:RC
Chief, Performance Improvement, Wage and Investment Division SE:W:S:PI
Program Manager, Automated Underreporter Program, Wage and Investment Division
SE:W:CP:RC:AUR
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
GAO/TIGTA Liaison, Deputy Commissioner for Operations Support OS
GAO/TIGTA Liaison, Deputy Commissioner for Services and Enforcement SE
GAO/TIGTA Liaison, National Taxpayer Advocate TA
GAO/TIGTA Liaison, Commissioner, Small Business/Self-Employed Division SE:S
Senior Operations Advisor, Wage and Investment Division SE:W:S



Appendix IV

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. These benefits will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Increased Revenue – Potential; \$2.2 million in additional tax assessments over 5 years could result if the Automated Underreporter function worked productive cases instead of repeatedly contacting taxpayers victimized by identity theft (see page 12).

Methodology Used to Measure the Reported Benefit:

We computed the potential increase in tax assessments if the Automated Underreporter function had worked more productive cases based on the 449 Tax Year 2004 cases closed as identity theft for the same underreported issues that were closed as identity theft in a prior year. We applied the IRS' reported \$980 average Automated Underreporter assessment per case to the 449 cases to arrive at \$440,020 (449 cases x \$980 per case) in assessments per year. If the IRS does nothing to correct the problem, we project approximately \$2.2 million (\$440,020 x 5 years) will be lost over 5 years.

Type and Value of Outcome Measure:

- Taxpayer Burden – Potential; 1,329 taxpayers were unnecessarily contacted multiple times by the IRS (see page 12).

Methodology Used to Measure the Reported Benefit:

We analyzed the Individual Master File¹ and a data extract of the Automated Underreporter system for Tax Years 2003 and 2004. We identified 633 taxpayers who were contacted multiple times by the Automated Underreporter function for the same underreported issues that were closed as identity theft in 2 or more years. We also found an additional 607 Tax Year 2005 cases that were still open as of March 2007 that may be closed as identity theft, and another 34 Tax

¹ The IRS database that maintains transactions or records of individual tax accounts.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

Year 2005 cases closed as “no change” after contacting the taxpayers for the same underreported issues that were closed as identity theft in a prior year.

We also analyzed the Individual Master File to identify taxpayers to whom the Withholding Compliance function had issued underwithholding letters. We matched those taxpayers to a data extract of the Automated Underreporter system for Tax Years 2003 and 2004. We found 55 taxpayers whose Tax Year 2003 cases the Automated Underreporter function had closed as identity theft who were subsequently contacted by the Withholding Compliance function for underwithholding problems resulting from the same identity theft issue.



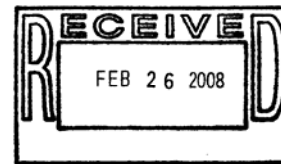
Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

Appendix V

Management's Response to the Draft Report




DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224



February 22, 2008

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Richard A. Spires 
Deputy Commissioner for Operations Support

SUBJECT: Draft Audit Report – Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft (Audit #200740004)

Thank you for the opportunity to respond to the referenced draft report. The IRS has made substantial progress in addressing identity theft since we first established our corporate identity theft strategy in November 2004. We continue to look for opportunities to make our efforts more effective and efficient in the areas of identity theft awareness, prevention, detection and prosecution.

To strengthen our enterprise-wide approach to identity theft, IRS established the Privacy, Information Protection, and Data Security (PIPDS) office in July 2007. PIPDS is led by a Senior Executive who reports directly to the Deputy Commissioner for Operations Support, which enables the office to reach across all IRS organizations and ensure that proper attention and discipline are given to the issues of privacy, identity theft, and data security. We created the Identity Theft and Incident Management (ITIM) office within PIPDS to continue implementing the IRS identity theft strategy and coordinate efforts within the IRS to provide assistance and consistent treatment to taxpayers who are victims of identity theft.

The IRS is also updating our identity theft strategy to reflect the implementation of several recommendations outlined in the President's Identity Theft Task Force¹ report for preventing and deterring identity theft. We have initiated efforts targeted to decrease the unnecessary use of Social Security Numbers (SSN), implement data security guidelines and rules, respond to data losses, and where appropriate, collaborate with law enforcement agencies to identify and prosecute identity theft.

¹ The President's Identity Theft Task Force, Combating Identity Theft, A Strategic Plan, April 2007.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

2

Your report highlighted some of the IRS' recent actions to tackle the identity theft problem through public outreach and victim assistance. However, we would like to draw attention to some additional accomplishments in combating identity theft that were not recognized in the report.

CI Activities Related to Tax Fraud Identity Theft Have Increased Substantially

In recent years, the IRS has devoted additional resources to detecting and investigating identity theft tax fraud. Our Special Agents in CI regularly collaborate with enforcement agencies that investigate identity theft, including the Federal Bureau of Investigation (FBI), the United States Secret Service (USSS), the United States Postal Inspection Services (USPIS), the Social Security Administration (SSA) Office of Inspector General (OIG), and the Department of Homeland Security (DHS).

CI's Fraud Detection Centers (FDCs) continue to improve ways to identify and analyze fraudulent tax refund schemes involving identity theft. Those returns meeting the appropriate criteria are forwarded to our field investigation offices to develop potential recommendations for prosecution.

The following table illustrates the substantial progress achieved by our CI FDCs. The number of returns identified as part of a refund crime has increased 589% from tax Processing Year (PY) 2005, when we identified 3,991 returns, to PY 2007, when we identified 27,513 returns. As a result, the amount of fraudulent identity theft refunds stopped has also increased substantially in each of the last three processing years.

Processing Year	PY 2005	PY 2006	PY 2007
Number of Returns	3,991	9,420	27,513
Total Dollars	\$ 20,924,948	\$ 76,977,587	\$213,114,294

CI Recommendations for Identity Theft Prosecutions

CI makes recommendations for prosecution of identity fraud using several statutes within CI's jurisdiction in addition to Title 18 USC 1028, the Identity Theft statute. Our policy is that alleged identity theft violations generally must have a strong nexus to a substantive tax offense involving significant amounts of revenue. This policy was derived in part because of the concerns raised in the April 1999 Webster Commission Report, which concluded that CI was experiencing "mission drift" in that a significant number of the cases it was investigating had only tangential connection to tax administration. Therefore, the



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

3

use of Title 18 USC 1028 is recommended to enhance egregious cases where substantive tax or money laundering violations (statutes over which CI has investigative jurisdiction) are being charged. These recommendations are approved by the Department of Justice (DOJ) and have a nexus to a tax crime.

The statutes listed below are routinely used by CI in cases involving identity theft and concentrate on the underlying tax crime and the resulting revenue loss to the government. They include:

- Title 18 USC 286 – Conspiracy to Defraud the Government with Respect to Claims
- Title 18 USC 287 – False, Fictitious, or Fraudulent Claims
- Title 18 USC 371 – Conspiracy to Commit Offense or to Defraud United States
- Title 26 USC 7201 – Attempt to Evade or Defeat Tax
- Title 26 USC 7203 – Willful Failure to File Return, Supply Information, or Pay Tax
- Title 26 USC 7206(1) and (2) – Filing False Returns and Aiding or Assisting in the Preparation of False Returns
- Title 18 USC 1956 and 1957 – Money Laundering

As you know, CI identifies identity theft cases largely through the Questionable Refund Program (QRP) and customarily addresses identity theft fraud within the traditional statutes within CI's jurisdiction. In the QRP, CI recommends prosecution primarily under Title 18 USC 286 (Conspiracy to Defraud the Government with Respect to Claims) and Title 18 USC 287 (False, Fictitious, or Fraudulent Claims). The average sentence for QRP investigations increased in FY 2007 from FY 2006, which is also an indication of the significance of these investigations. CI also recommended 45 prosecutions in Fiscal Year (FY) 2005 and 55 prosecutions in FY 2006 under the identity theft statute, Title 18 USC 1028. When taking into consideration all of the statutes within CI's jurisdiction under which identity theft has been traditionally charged, the percentage of overall prosecutions increases dramatically from the numbers illustrated in Figure 2 of your report.

Each prosecution recommendation under Title 18 USC 1028, the Identity Theft statute, has a wide reaching impact on the number of false returns/potential victims and the resulting impact on tax administration. Upon further review of these prosecution recommendations, we were able to identify the number of false returns/potential victims associated with each. There were 5,775 false returns/potential victims associated with the 45 prosecution recommendations in FY 2005, and 3,105 false returns/potential victims associated with the 55 prosecution recommendations in FY 2006.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

4

Sources of Information Including Referrals and the FTC Clearinghouse

CI evaluates and employs a wide variety of information sources to identify potential identity theft fraud and to support recommendations for prosecutions. CI regularly collaborates with various state, federal, and local law enforcement agencies that investigate identity theft crimes, as well as receives leads from private entities and members of the public, which they act upon. These activities are in addition to addressing internal fraud referrals from various other IRS functions, including Automated Underreporter (AUR), and Field Examination functions which totaled 625 in FY 2005 and 603 in FY 2006. These internal fraud referrals may or may not include identity theft.

As you know, the FTC's Identity Theft Data Clearinghouse is a secure online database of millions of consumer fraud and identity theft complaints and is available only to Law Enforcement in the course of pursuing an identity theft investigation. The PIPDS office has recently engaged the FTC to initiate opportunities to collaborate in outreach activities. We have received extracts of general information from the Clearinghouse, inclusive of all tax administration identity theft, to track trends and develop process improvement and outreach initiatives for victim assistance.

We recently evaluated a sample of the complaints in the FTC Identity Theft Data Clearinghouse marked as "Fraudulent Tax Return Filed". In the complaints reviewed by CI, the data generally did not provide enough details or personal information needed to support the initiation of an investigation for a federal criminal tax prosecution. Additionally, even the FTC's own publication, the *Consumer Sentinel*, states, "[t]he consumer's personal information and information about the suspect are not verified or authenticated by the FTC's Identity Theft Program. Therefore, it should not be relied upon without additional investigation."² For these reasons, CI generally relies upon alternative data sources to support specific cases where CI recommends criminal tax prosecutions.

Employment-related Identity Theft

IRS recognizes the additional taxpayer burden that is created when both the name and SSN of a taxpayer are used unlawfully by an identity thief to gain employment. In these cases, the victim may be contacted by our Compliance function to report the wages earned by the identity thief and reported to IRS by the third party payer or employer.

² The Consumer Sentinel is a secure online database maintained by the FTC that includes consumer fraud and identity theft complaints available only to Law Enforcement.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

5

As you know, the IRS is prohibited from notifying the employer when, in the course of carrying out one of our business processes, we learn that wage information reported to IRS using the victim's name and SSN is not accurate. Section 6103 of the Internal Revenue Code generally restricts the IRS from sharing taxpayer or tax return information with third parties. This restriction applies to the sharing of Form W-2 information with employers or with other Government agencies, except in very limited circumstances.

Nonetheless, we have several actions in process which will further reduce the burden to the victim in these cases. One of our new compliance letters also includes advice to these taxpayers about contacting the third party payer to correct their records. These letters inform the taxpayers that the information reported to the IRS by third party payers, such as employers, financial institutions, etc., is different from the information reported on his or her tax return.

Targeted Enforcement Initiatives to Be Led by SSA OIG and DHS

As you stated in your report, the President's Task Force on Identity Theft recommends that law enforcement agencies continue to conduct enforcement initiatives that focus exclusively or primarily on Identity theft. Furthermore, the Task Force designates the SSA OIG and DHS as the lead agencies to address targeted enforcement initiatives for employment-related identity theft.

"Law enforcement agencies should continue to conduct enforcement initiatives that focus exclusively or primarily on identity theft. The initiatives should pursue the following:

- Unfair or Deceptive Means to Make SSNs Available for Sale. - Beginning immediately, law enforcement should more aggressively target the community of businesses on the Internet that sell individuals' SSNs or other sensitive information to anyone who provides them with the individual's name and other limited information. The SSA OIG and other agencies also should continue or initiate investigations of entities that use unlawful means to make SSNs and other sensitive personal information available for sale.
- Identity Theft By Illegal Aliens. Law enforcement agencies, particularly the Department of Homeland Security, should conduct targeted enforcement initiatives directed at illegal aliens who use stolen identities to enter or stay in the United States."

The Deputy Commissioner for Operations Support will coordinate with the Deputy Commissioner of Services and Enforcement as we continue to work with these lead agencies to address this issue and implement the Task Force recommendations.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

6

IRS Has Made Substantial Improvements to the AUR Program to Reduce Burden on Identity Theft Victims

The IRS began addressing identity theft in the AUR program in FY 2005. Identity theft cases are identified in the AUR program after a taxpayer receives a notice from the IRS that he or she has not reported all income on the return, such as wages on Form W-2. After the taxpayer self-identifies as an identity theft victim, AUR will request documentation from the taxpayer to verify his or her identity and to affirm that the wages or other income in dispute were not received by the taxpayer. If the impacted taxpayer provides the IRS with the necessary documentation, the IRS will not assess the additional tax from the unreported income. The IRS also shares the corrected information with the SSA to assist in updating the taxpayer's total wages and Social Security taxes reported to the SSA.

Closing codes were developed to place on these accounts where the taxpayer provides the documentation confirming that the income was incorrectly reported under their SSN. To further reduce taxpayer burden, AUR developed an account indicator in FY 2007 to exclude these cases from the AUR inventory.

Beginning in January 2008, the IRS started closing all verified identity theft cases with a universal identity theft indicator. The universal identity theft indicator and the closing codes will be used as factors in the selection and prioritization of AUR cases in future years. We expect that this process will substantially reduce the number of cases when the IRS contacts the taxpayer multiple times.

IRS' Implementation of a Universal Identity Theft Indicator

The IRS understands the enormous burden placed on individuals who are the victims of identity theft, and we are working diligently to minimize this burden. In collaboration with representatives from IRS business and operating divisions, the IRS implemented in January 2008 the use of a universal identity theft indicator (TC971, Action Code 501).

The PIPDS office has realized substantial progress with implementing the universal identity theft indicator in 2007. We worked with all business units that are impacted by identity theft in tax administration to ensure consistent application of the universal identity theft indicator. This process includes the development of business rules for various programs, among these are CI Refund Crimes, AUR, and Withholding Compliance, to apply unique treatments to these cases when this indicator is present. As part of this effort, the ITIM office within PIPDS is also reviewing business unit Internal Revenue Manual guidelines, conducting one-on-one support sessions with business unit staff, and communicating with business unit executives.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

7

The universal identity theft indicator provides the IRS with comprehensive data from all program areas impacted by identity theft, giving us a tool to determine the impact that identity theft has on tax administration. As your report notes, the indicator facilitates the tracking of identity theft, the protection of Treasury revenue threatened by identity fraud, and the reduction of taxpayer burden related to identity theft and several business units are actively applying this code. As of February 16, 2008 we have applied the indicator to 887 accounts since the code became available in January 2008.

RECOMMENDATION 1

The Deputy Commissioner for Operations Support should coordinate with the Deputy Commissioner for Services and Enforcement to develop and implement a strategy to address employment-related and tax fraud identity theft.

CORRECTIVE ACTION

We agree that the aggressive pursuit of identity theft criminals is a deterrent to identity theft. We created our original strategy to address outreach, victim assistance and prevention in November 2005. As we stated earlier in our response, we will continue to update our strategies to make our efforts more effective and efficient in the areas of identity theft awareness, prevention, detection and prosecution. We are in the process of developing our vision for the future of the PIPDS organization and priorities and are documenting this 5 year strategy in our Concept of Operations (CONOPS). The Deputy Commissioner for Operations Support will continue to work with the Deputy Commissioner for Services and Enforcement to continuously improve IRS' strategies focused on tax fraud identity theft. Our Criminal Investigation (CI) division is actively working with the Privacy, Information Protection, and Data Security (PIPDS) office on several initiatives to detect tax fraud identity theft, identify the victims, and provide them with assistance. Recent efforts include the notification of taxpayers who have been identified as victims of a tax fraud identity theft where someone may have attempted to impersonate them by using their personal information to file a tax return. We are providing these victims with information about the resources available for them to monitor their financial accounts and about other actions they can take to protect themselves in the future.

CI is also vigorously increasing the recommendations for prosecutions of identity theft cases under traditional statutes within IRSs jurisdiction as directed by the Department of Justice (DOJ) Tax Division. When taking into account the recommendations for prosecutions for all identity theft cases under all statutes available for prosecution, it is clear that the IRS is taking an active role in pursuing identity theft criminals.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

8

Our position on employment-related identity theft remains the same as stated in previous testimony. We do not agree with your statements recommending that IRS more actively try to identify or stop the individuals from committing employment related identity theft and notify the employer of the problem of their employee using someone else's identity. As former Commissioner Everson testified in a March 2004 hearing before the House Ways and Means Subcommittee on Oversight and Social Security, notwithstanding that many employees may not be authorized to work in the United States, the IRS is broadly restricted under Section 6103 of the Internal Revenue Code (IRC) from sharing taxpayer information with third parties, including employers, except in very limited circumstances.

This taxpayer information includes the possibility that the employee is not working legally in the United States or is using an SSN that does not belong to him or her. This restriction prevents the IRS from notifying an employer that one of their employees may be unlawfully using another person's name and Social Security Number to gain employment. Though we have no legal authority with respect to the enforcement of immigration and social security administration laws, the IRS remains legally responsible for enforcement of the nation's Federal tax laws with respect to all workers, including the responsibility to assess and impose tax on workers irrespective of the circumstances of their employment. For this reason, we have focused our efforts on reducing the burden to the victims of employment related identity theft.

An electronic copy of your report was shared with the Office of the Assistant Secretary for Tax Policy which is responsible for proposing legislative changes to evaluate your recommendation for a legislative remedy to expand the exceptions to IRC Section 6103.

The President's Identity Theft Task Force report provides a comprehensive approach for combating identity theft and outlines strategies for addressing employment-related identity theft. The Task Force identified the Social Security Administration (SSA) Office of Inspector General (OIG) and the Department of Homeland Security (DHS) as the lead agencies to address this issue, and the Deputy Commissioner for Operations Support will coordinate with the Deputy Commissioner of Services and Enforcement as we work with these agencies to implement the Task Force recommendations. The PIPDS office will continue to reach out to key stakeholders such as the FTC, SSA OIG, and DHS to update our strategies to address employment-related identity theft. We will actively implement on any solutions that are within our scope and approved by the IRS Senior Leadership.

In addition, the IRS has taken several actions to reduce the burden to the victim in these cases. The IRS has included additional advice in some of the underreporter letters advising these taxpayers to contact the employers to allow the employer to correct their records.



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

9

IMPLEMENTATION DATE

N/A

RESPONSIBLE OFFICIAL

N/A

CORRECTION ACTION MONITORING PLAN

N/A

RECOMMENDATION 2

The Deputy Commissioner for Operations Support should coordinate with the Deputy Commissioner for Services and Enforcement to:

- Update the individual case screens on the Automated Underreporter system to display prior year closing codes.
- Ensure revision of the Withholding Compliance function case selection criteria to incorporate special handling of identity theft victims.

CORRECTIVE ACTION

We agree that IRS should continue to seek opportunities to improve our business processes and technology systems in order to further reduce taxpayer burden and eliminate multiple contact of identity theft victims. The solution we have already implemented supersedes the need to update the individual case screens on Automated Underreporter (AUR) to display prior year closing codes. Beginning in January 2008, the IRS implemented the use of a universal identity theft indicator (TC971, Action Code 501), which is placed on a taxpayer's account when the taxpayer self-identifies as an identity theft victim and provides the IRS with the proper documentation to verify his or her identity. The use of this code standardizes the identification and tracking of identity theft accounts across multiple tax modules in all IRS functions. In addition, the IRS will develop business rules for various programs, including Criminal Investigation Refund Crimes, AUR, and Withholding Compliance, to apply unique treatments to cases when this indicator is present.

IMPLEMENTATION DATE

N/A

RESPONSIBLE OFFICIAL

N/A

CORRECTIVE ACTION MONITORING PLAN

N/A



Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft

10

RECOMMENDATION 3

The Deputy Commissioner for Operations Support should coordinate with the Deputy Commissioner for Services and Enforcement to establish closing codes for multiple issue cases on the Automated Underreporter system that will allow for individual underreporting issues to be closed as identity theft.

CORRECTIVE ACTION

We agree that additional information about identity theft cases is needed to determine the impact of identity theft on tax administration. To gather this data, the IRS implemented, in January 2008, the universal identity theft indicator on the Individual Master File. The purpose of this indicator is to centrally track incidents of identity theft, protect Treasury revenue threatened by identity fraud, and reduce taxpayer burden related to identity theft.

The universal identity theft indicator (TC971, Action Code 501) is placed on a taxpayer's account when the taxpayer self-identifies as an identity theft victim and supersedes the need for the Automated Underreporter program to develop a new system to report multiple closing codes. As we stated earlier in our response, the universal identity theft indicator and the closing codes will also be used as factors in the selection and prioritization of AUR cases in future years.

IMPLEMENTATION DATE

N/A

RESPONSIBLE OFFICIAL

N/A

CORRECTIVE ACTION MONITORING PLAN

N/A