

September 2009

TAX ADMINISTRATION

IRS Has Implemented Initiatives to Prevent, Detect, and Resolve Identity Theft-Related Problems, but Needs to Assess Their Effectiveness



GAO

Accountability * Integrity * Reliability



Highlights of [GAO-09-882](#), a report to congressional requesters

Why GAO Did This Study

Identity thieves may use a taxpayer's name and social security number to fraudulently claim a refund or gain employment. This creates tax problems for the innocent taxpayer when the Internal Revenue Service (IRS) discovers a duplicate refund claim or unreported wage income. IRS is revising its strategy for preventing, detecting, and resolving identity theft-related tax problems.

GAO was asked to (1) describe the extent of identity theft-related refund and employment fraud, (2) assess IRS's actions to prevent and resolve such problems, and (3) describe IRS's identity theft-related coordination with other agencies. GAO analyzed IRS data on identity theft cases, reviewed revisions to the Internal Revenue Manual and other agency documents, and interviewed IRS officials responsible for the new strategy.

What GAO Recommends

GAO recommends that IRS ensure that performance measures suitable for assessing the effectiveness of its identity theft initiatives, and associated data collection procedures, are in place at the beginning of the 2010 filing season. IRS agreed with GAO's recommendation and provided comments on technical issues, which we incorporated into this report where appropriate.

View [GAO-09-882](#) or [key components](#). For more information, contact James R. White at (202) 512-9110 or whitej@gao.gov.

TAX ADMINISTRATION

IRS Has Implemented Initiatives to Prevent, Detect, and Resolve Identity Theft-Related Problems, but Needs to Assess Their Effectiveness

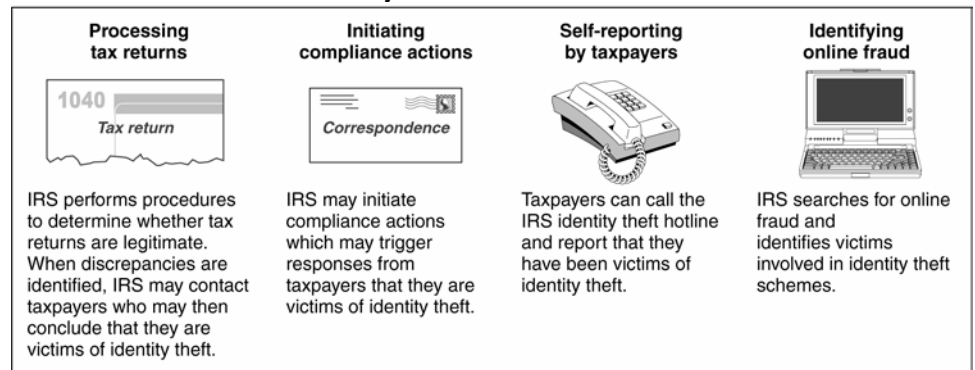
What GAO Found

IRS's ability to detect identity theft-related refund and employment fraud is limited, but by the end of 2008, IRS had cataloged over 50,000 incidents. According to IRS, about 90 percent of fraudulently claimed refunds were stopped in 2008 with about \$15 million issued before IRS became aware of the fraud. IRS does not know the amount of refund or employment fraud that goes undetected.

In 2008, IRS began implementing four new initiatives in an effort to better detect and resolve identity theft cases. These include an identity theft indicator that IRS places on victims' accounts so that IRS personnel can more easily recognize and assist the legitimate taxpayer in case of future account problems. The indicator further enables IRS to screen returns to prevent fraudulent refunds from being issued to identity thieves. IRS also decided to resolve legitimate taxpayers' identity theft problems using a decentralized process—the activity that discovers a problem has the responsibility to resolve it. For the 2010 filing season, IRS is considering whether to expand its screening; however, IRS does not know how well its current strategy is working. IRS said it will develop performance measures, but it is not known whether the measures will be suitable for determining the effectiveness of the new initiatives, such as the number of false positives and negatives in the screening process or the success of the decentralized resolution process. Nor is it known when the new measures will be implemented. Measuring effectiveness matters because there have been glitches in implementing the initiatives. IRS is working to correct some discrepancies in the screening process and a GAO analysis of IRS data showed that some fraudulent refunds were issued even though taxpayers had indicators on their accounts.

IRS's coordination with other agencies is limited. Statutory Provisions protecting the privacy of tax data prohibit IRS from sharing taxpayer information with other agencies in many cases. Nor does IRS routinely receive identity theft case data because of concerns with substantiation. IRS has coordinated with other agencies on how to manage identity theft programs.

Processes IRS Uses to Detect Identity Theft



Sources: GAO analysis of IRS information; Art Explosion (clip art).

Contents

Letter		1
	Background	3
	IRS's Ability to Detect and Catalog Current Identity Theft Incidents Is Limited and the Amount That Goes Undetected Is Not Known	7
	IRS Has Implemented New Initiatives in an Effort to Detect and Resolve Identity Theft Cases, but Not Enough Is Known about How Well the Initiatives Are Working	11
	Privacy and Other Laws Limit IRS's Coordination with Other Agencies on Identity Theft Cases	20
	Conclusion	22
	Recommendation for Executive Action	23
	Agency Comments	23

Appendix I	Objectives, Scope, and Methodology	25
-------------------	---	----

Appendix II	Description of Indicator Codes Used to Identify Tax and Non-Tax Related Issues	28
--------------------	---	----

Appendix III	Procedures Followed for Additional Screening of Certain Indicator Accounts	29
---------------------	---	----

Appendix IV	Comments from the Internal Revenue Service	30
--------------------	---	----

Appendix V	GAO Contact and Staff Acknowledgments	31
-------------------	--	----

Tables

Table 1: Number of Verified Identity Theft Cases by IRS Activity Cataloged by December 31, 2008 (encompassing multiple tax years)	8
Table 2: Number of Verified Identity Theft Cases by Type of Fraud, Cataloged as of December 31, 2008	9

Table 3: Suspected Identity Theft-Related Refund Fraud Identified and Stopped by IRS, Calendar Year 2008	10
Table 4: Numbers of Incidents and Taxpayers with Identity Theft-Related Indicators Cataloged as of December 31, 2008 (encompassing multiple tax years for 501 and 506 indicators)	12
Table 5: Percentage of Suspected Identity Theft Refunds Stopped and Issued by IRS When Indicators Were on the Taxpayers' Accounts, Partial Calendar Year 2009	16
Table 6: Indicator Codes Used by IRS to Flag Taxpayer Accounts for Tax- and Non-Tax-Related Identity Theft Issues	28

Figures

Figure 1: Processes IRS Uses to Detect Identity Theft	4
Figure 2: Total Identity Theft Complaints Received by the FTC, 2004–2008	6
Figure 3: Number of Fraudulent Web Sites Taken Down, 2006–2009	18
Figure 4: Process Followed to Run Tax-Related Accounts with Indicator Codes through Additional Screening Procedures	29

Abbreviations

CI	Criminal Investigation Division
DHS	Department of Homeland Security
DOJ	Department of Justice
FTC	Federal Trade Commission
IPSU	Identity Protection Specialized Unit
IRC	Internal Revenue Code
IRS	Internal Revenue Service
OFDP	Online Fraud Detection and Prevention
PIPDS	Office of Privacy, Information Protection and Data Security
QRP	Questionable Refund Program
SB/SE	Small Business/Self-Employed Division
SSA	Social Security Administration
SSN	Social Security Number
SAS	Statistical Analysis Software
TAS	Taxpayer Advocate Service
TC	Transaction Code
TIGTA	Treasury Inspector General for Tax Administration
W&I	Wage and Investment Division

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

September 8, 2009

The Honorable Max Baucus
Chairman
The Honorable Charles E. Grassley
Ranking Member
Committee on Finance
United States Senate

The Honorable John Lewis
Chairman
The Honorable Charles W. Boustany, Jr.
Ranking Member
Subcommittee on Oversight
Committee on Ways and Means
House of Representatives

Identity theft is a serious and growing problem in the United States. According to the Federal Trade Commission (FTC), millions of people have been victims of the crime, some of whom may go years without knowing it. The crime takes many forms; identity thieves may obtain a credit card, rent an apartment, or establish a telephone account in the theft victim's name. The victim may not find out about the theft until being contacted by a debt collector, losing out on a job opportunity, or being denied a loan. Identity theft creates two main problems for taxpayers and IRS. A taxpayer may have his or her tax refund delayed if an identity thief files a fraudulent tax return seeking a refund using the legitimate taxpayer's name and Social Security number (SSN). In addition, a taxpayer may become subject to Internal Revenue Service (IRS) enforcement actions after someone else uses his or her identity to fraudulently obtain employment and the identity thief's income is reported to IRS by an employer on a Form W-2 (Wage and Tax Statement) or Form 1099 information returns in his or her name.

In 2004, IRS developed a strategy to address the problem of identity theft-related tax administration issues. According to IRS, the strategy has evolved and continues to serve as the foundation for all of IRS's efforts to provide services to victims of identity theft and to reduce the effects of identity theft on tax administration. The original strategy was revised in July 2008 and renamed IRS's Identity Protection Strategy by the Office of Privacy, Information Protection and Data Security (PIPDS), created by IRS to reach across all IRS organizations on issues of privacy, identity theft,

and data security. The IRS strategy focuses on three priority areas that are fundamental to addressing the identity theft challenge: victim assistance, outreach, and prevention.

In this context, you asked us to assess IRS's efforts to address the impact of identity theft on taxpayers. The objectives of this report are to (1) describe how much identity theft-related refund and employment fraud IRS faces and whether incidents of identity theft go undetected by IRS, (2) assess the actions IRS is taking to prevent and detect identity theft-related tax problems and to assist affected taxpayers, and (3) describe what IRS is doing to coordinate its identity theft-related efforts with those of other government and nongovernment entities.

To meet our objectives, we analyzed IRS data on identity theft cases, reviewed documentation on IRS's identity theft strategy, and interviewed responsible IRS executives. More specifically, we reviewed documents on policies and procedures related to identity theft and relevant sections of the Internal Revenue Manual and interviewed officials from PIPDS, Wage and Investment Division (W&I), Small Business/Self-Employed Division (SB/SE), and Criminal Investigation Division (CI) to determine the processes and procedures used by IRS to prevent and detect identity theft-related tax issues and assist affected taxpayers. We also reviewed prior GAO and Treasury Inspector General for Tax Administration (TIGTA) reports on these procedures. We also reviewed IRS's Identity Protection Strategy. To assess whether IRS's initiatives were working as intended, we obtained data from the Taxpayer Advocate Service (TAS) and IRS to identify (1) the frequency with which suspected identity theft-related refund fraud reoccurred for taxpayers known to have had identity theft issues in the past and (2) how often taxpayers took identity theft-related tax problems to TAS after other IRS functions had determined that their issues were identity theft-related. We determined that the IRS data that we used for this analysis were sufficiently reliable for our purposes. We also interviewed PIPDS officials and reviewed PIPDS documents to obtain information on IRS's coordination efforts with law enforcement and other government entities. Detailed information about our methodology can be found in appendix I. We conducted this performance audit from October 2008 through August 2009 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

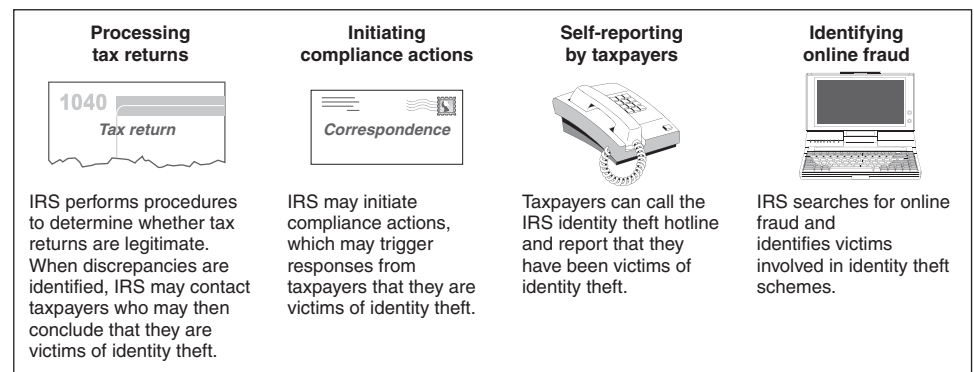
Identity theft describes a wide range of types of theft and uses of stolen information. According to the FTC, the most common form of identity theft is the use of another person's information to obtain credit and then acquire goods or services, not pay for them, and thus damage the credit rating of the identity theft victim.

As already noted, identity theft most commonly becomes a tax administration problem for victims and IRS in two primary ways. First, an identity thief may use a legitimate taxpayer's identity to fraudulently file a tax return and claim a refund during the filing season. In these cases, the identity thief typically uses a stolen SSN to file a forged tax return and obtain a refund early in the filing season. The legitimate owner of the SSN may not be aware that this has occurred until he or she files a tax return later in the filing season and IRS discovers that two returns have been filed using the same SSN. In this instance, the legitimate taxpayer's refund will likely be frozen until IRS can determine the legitimate owner of the SSN. The second way that identity theft becomes a problem for taxpayers and for IRS is through employment fraud. This occurs when an identity thief uses someone else's name and SSN to obtain a job. In this instance, IRS would receive a Form W-2 or a Form 1099 reporting income on the taxpayer's account, which the rightful owner of the SSN had not earned and does not report as income to IRS. As a result, the taxpayer may be subject to enforcement action when, during the filing process, IRS matches what the employer and the taxpayer report and it appears that he or she earned more income than was reported on his or her tax return. In a related type of case, an identity thief uses just the SSN of a legitimate taxpayer and the thief's own or a made up name. This also creates tax administration problems (as well as problems for the Social Security Administration) because the same SSN is now associated with multiple names. The name and SSN information used by identity thieves to commit refund or employment fraud are typically stolen from sources beyond the control of IRS. In many cases, the source of the stolen information is unknown. Someone who makes up an SSN that does not match a legitimate SSN and uses it to gain employment has failed to comply with legal requirements to supply a valid SSN but has not committed identity theft because no person's identity was stolen.

Identity theft can also involve IRS in other ways, such as when thieves masquerade as IRS in order to steal information over the Internet through phishing schemes—using e-mail or Web sites to impersonate IRS and ask for personal and financial information from unsuspecting victims. According to IRS, there are a variety of online schemes that victimize taxpayers. "Get Your Refund" phishing e-mails appear to be legitimate e-

mails from IRS notifying a taxpayer that they are entitled to a refund and can claim it quickly by clicking on a fraudulent link within the e-mail and providing their personally identifiable information. Fraudulent free e-file Web sites claim to be legitimate free e-file Web sites. Once a taxpayer enters his or her tax information, the identity thief enters his or her own bank account number and then steals the refund along with the taxpayer's personal information, such as the SSN. Other schemes include surveys and malware.¹ Surveys are usually sent through e-mails, where the fraudulent party masquerades as IRS asking taxpayers to rate their experience with IRS. Malware is an executable file sent through an e-mail, which asks the recipient to save and run a file. Once the file runs, information is pulled from the victim's computer and sent to the fraudulent party. Identity theft can also involve IRS when IRS loses taxpayer data in either electronic form, such as information stored on a lost laptop computer, or on paper, such as documents lost in transit when being sent from one IRS facility to another. However, lost taxpayer data will not result in identity theft unless the data were found by an identity thief who uses the data for personal gain. Figure 1 describes the ways that identity theft issues come to light for IRS and taxpayers.

Figure 1: Processes IRS Uses to Detect Identity Theft



Sources: GAO analysis of IRS information; Art Explosion (clip art).

Federal and state legislatures have toughened laws that prohibit the theft of identities. In October 1998, Congress passed the Identity Theft and

¹Malware (malicious software) is defined as programs that are designed to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs so that users are induced into activating them.

Assumption Deterrence Act,² which expanded the criminalization of fraud in connection with identification documents to cover the unlawful transfer and use of identification documents. The law addresses identity theft by including instances 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.” According to the President’s Identity Theft Task Force, all 50 states and the District of Columbia have some form of legislation that prohibits identity theft, and in all of those jurisdictions, except Maine, identity theft can be prosecuted as a felony.

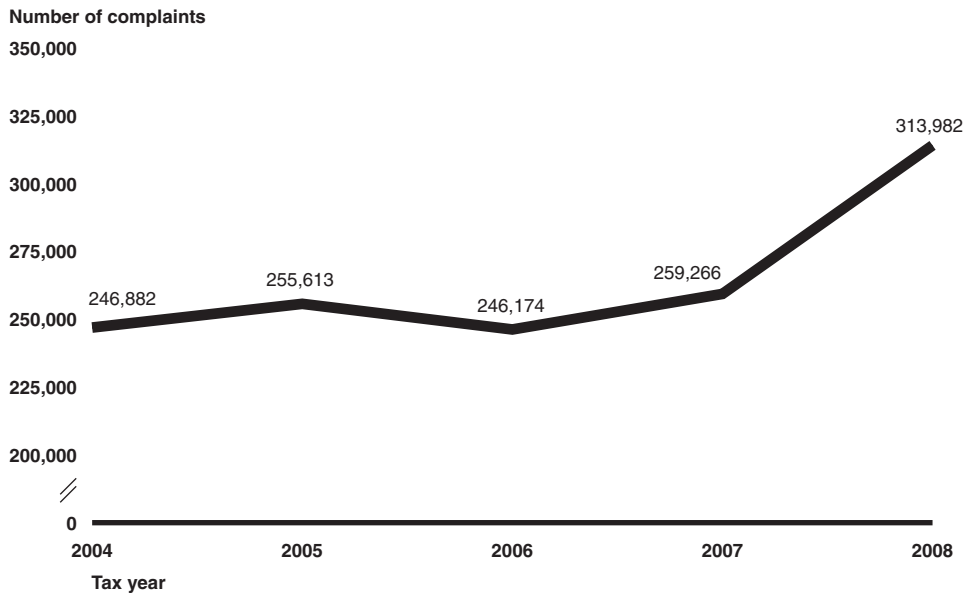
In addition to congressional efforts to combat identity theft, there have been administrative efforts as well. The President’s Identity Theft Task Force was established in May 2006 by Executive Order 13402.³ The task force was created to coordinate federal agencies in their efforts against identity theft and to create a strategic plan to combat (increase awareness of, prevent, detect, and prosecute) identity theft.

Victims of identity theft can file a complaint with the FTC. The FTC maintains an Identity Theft Data Clearinghouse, which is the sole national repository of consumer complaints on identity theft. In 2008, the FTC received 313,982 identity theft complaints, a large increase over the number reported in prior years, as shown in figure 2.

²Pub. L. No. 105-318, 112 Stat. 3007 (1998).

³Exec. Order No. 13,402 (May 10, 2006), 71 *Fed. Reg.* 27,945 (May 15, 2006).

Figure 2: Total Identity Theft Complaints Received by the FTC, 2004–2008



Source: GAO analysis of FTC data.

Intending to strengthen IRS’s enterprisewide approach to identity theft and data security, IRS established PIPDS in July 2007. PIPDS includes four offices with roles defined by IRS as follows:

- **Privacy.** Promotes the protection of individual privacy and integrates privacy into business practices, behaviors, and technology solutions.
- **Identity Protection.** Identifies risks and reduces vulnerabilities of identity information, enhances services and reduces burden and harm to identity theft victims, and increases collaboration and communication with IRS stakeholders and external partners.
- **Incident Management.** Assesses and reduces IRS data loss incidents, promotes protection of personal identity information by IRS employees, and informs taxpayers of identity theft risks discovered by the IRS.
- **Online Fraud Detection and Prevention.** Reduces and prevents online fraud against IRS and taxpayers.

PIPDS collaborates with IRS activities⁴ that deal with identity theft cases and issues. A technical working group was formed to provide a forum for

⁴We are defining activities to include IRS business operating divisions, functions, or programs.

developing recommendations on how processes and procedures can be improved to address and reduce the burden on taxpayers who are victims of identity theft. Additionally, IRS established two advisory committees to oversee Identity Theft and Incident Management and Online Fraud Detection and Prevention activities. The advisory committees include executive management from Small Business/Self-Employed (SB/SE), Wage and Investment (W&I), Criminal Investigation (CI), and the Taxpayer Advocate Service (TAS).

IRS's Ability to Detect and Catalog Current Identity Theft Incidents Is Limited and the Amount That Goes Undetected Is Not Known

IRS began systemically cataloging data on identity theft incidents in January 2008, but limitations on the data mean that the data provides an incomplete picture of the amount of identity theft-related fraud occurring at IRS. IRS catalogs identity theft incidents after identifying a possible case, validating that identity theft-related fraud occurred, and substantiating the identity of the victim taxpayer. Because of the timing of tax return filing, IRS is often unable to detect suspicious cases until well after the fraud occurred. Validating the identity theft and substantiating the victim's identity takes further time. For example, IRS may not be able to detect potential employment fraud until after the following year's tax filing deadline of April 15 when it matches Form W-2 information against filed tax returns. It is only after IRS notifies a taxpayer of unreported income that IRS may learn from the taxpayer that the income was not his or hers and that someone else must have been using his or her identity. By the time both the victim and IRS determine that an identity theft incident occurred, well over a year may have passed since the employment fraud.⁵

Time lags are not the only issue obscuring a complete picture of identity theft tax cases at IRS. Some cases go undetected altogether. One reason for this is that IRS does not investigate every case of potential employment fraud. Because of the large volume of mismatches between what is reported on a Form W-2 or a Form 1099 information return and what is reported on an income tax return, and also because of IRS's limited resources, IRS does not pursue some mismatches. Consequently, IRS is not in a position to detect any underlying identity theft in those cases. Also, if an identity thief steals the identity of a person with no tax filing obligation, such as a child, and files returns and pays taxes using the name

⁵Another reason a catalog of identity theft incidents is incomplete is because not all victims decide to substantiate the identity theft; IRS only catalogs a case if the victim is able to substantiate the theft.

and SSN of that person, IRS may have no way of detecting the identity theft. From IRS's point of view, a tax return has been filed with a name and SSN that match and the income on the tax return matches income reported by an employer.

Many IRS Activities Detected Identity Theft

Table 1 shows the tax-related identity theft incidents that IRS cataloged as of December 31, 2008. Most of the incidents in the table are for identity thefts that occurred since 2005, but some incidents go back many years.

The incidents shown in table 1 include open tax-related identity theft cases reported by various IRS activities. A case is considered open if the taxpayer continues to have identity theft-related issues. For all of the incidents shown in table 1, IRS validated that the identity theft-related fraud occurred and substantiated the identity of the victim taxpayer. The table demonstrates that IRS detects identity theft throughout the course of normal tax administration activities, including processing tax returns, examining returns to verify compliance, and collecting tax debt.

Table 1: Number of Verified Identity Theft Cases by IRS Activity Cataloged by December 31, 2008 (encompassing multiple tax years)

IRS activity	Number of incidents ^a	Number of taxpayers affected
Criminal Investigations: Investigates questionable refunds and fraudulent refund schemes.	17,836	16,696
Automated Underreporter: Compares amounts reported by third parties to amounts reported on individual income tax returns.	10,536	9,527 ^b
Field Assistance: Provides face-to-face assistance to taxpayers at Taxpayer Assistance Centers.	10,792	7,671 ^b
Accounts Management: Responds to taxpayer inquiries and works to resolve cases of duplicate tax returns.	3,486	2,691 ^b
Taxpayer Advocate Service: Assists taxpayers who are experiencing economic harm or seeking help in resolving tax problems that have not been resolved through normal channels.	2,308	1,827 ^b
Correspondence Exam: Conducts audits of individual tax returns by mail.	1,549	1,434 ^b
Automated Substitute for Return: Creates a substitute tax return where none was filed and makes a tax assessment.	2,621	1,304 ^b
Automated Collection System: Contacts taxpayers by telephone to collect and resolve delinquent tax cases.	1,709	983 ^b
Compliance Service Collections Operations: Contacts taxpayers by correspondence to collect and resolve delinquent tax cases.	828	492 ^b
Other ^c	37	32 ^b

Source: GAO analysis of IRS data.

^aThe number of incidents of identity theft is higher than the number of taxpayers because a taxpayer can have more than one incident of identity theft.

^bA taxpayer may have been identified as a victim of identity theft through different tax administration activities in different tax years by different IRS activities; therefore, a taxpayer may be counted more than once. According to IRS data, the total number of taxpayers double counted was 1,779.

^cOther includes Field Examination, Field Collection, and Office of Privacy and Information Protection.

The 51,702 incidents cataloged in table 1 are primarily refund or employment fraud, as shown in table 2.

Table 2: Number of Verified Identity Theft Cases by Type of Fraud, Cataloged as of December 31, 2008

Type of fraud	Number of incidents	Number of taxpayers affected ^a
Refund fraud	23,124	21,047
Employment fraud	24,925	17,645
Both	1,036	793
Other ^b	2,617	2,016

Source: GAO analysis of IRS data.

^aA taxpayer may be counted more than once if he or she has been identified as a victim of identity theft through different IRS activities or in different time periods. According to IRS data, the number of taxpayers double counted was 623.

^bThe "Other" category includes identity theft incidents that cannot be identified as related to any current year tax administration issue, such as issues that occurred in tax year 2007 but were not detected until 2008.

IRS identifies refund fraud primarily through the Questionable Refund Program (QRP) in CI. QRP was established to identify fraudulent returns, stop the payment of fraudulently claimed refunds, and, in some cases, refer fraudulent refund schemes to CI's field investigation offices. CI may ultimately refer refund schemes to the Department of Justice (DOJ) for possible criminal prosecution. According to data from CI, the median amount of suspected identity theft-related refunds identified during the 2009 filing season was about \$3,400.⁶

Over the past 4 years, CI has investigated a number of tax-related identity theft cases that DOJ successfully prosecuted. For example, a former Girl Scout troop leader is now serving 10 years in federal prison for using children's identities to defraud the government. The defendant pleaded guilty to multiple counts of filing fictitious tax refund claims and identity theft. The defendant created fake medical release forms for her troop members and told their parents that she needed the girls' SSNs in case of

⁶CI provided data on fraudulent refunds stopped and issued from January 1, 2009, to April 30, 2009, and about \$3,400 is the median amount from these data.

an emergency. The scheme helped her claim more than \$87,000 in fraudulent tax refunds.

According to CI data, in 2008, IRS stopped about 90 percent of suspected identity theft-related refunds it identified as shown in table 3.⁷ For the other 10 percent, a majority of the refunds were issued to suspected identity thieves before the legitimate taxpayer filed their return. It is only when IRS finds a duplicate tax return (a second return filed using the same name and SSN) that IRS has an indication of potential refund fraud.

Table 3: Suspected Identity Theft-Related Refund Fraud Identified and Stopped by IRS, Calendar Year 2008

	Number	Dollars
Fraudulent tax returns identified by IRS	30,328	\$179,129,228
Fraudulent tax returns stopped by IRS	26,385	\$163,819,228
Percent stopped	87	91

Source: GAO analysis of IRS data.

Note: Not all tax returns identified were verified as identity theft related during 2008.

As shown in table 3, about \$15 million in fraudulent refund payments were issued in calendar year 2008. IRS officials said that they could not determine how many of those refunds have been recovered. They said that in instances where CI opens a criminal investigation and the government successfully prosecutes the identity thief, upon conviction the perpetrator may be ordered by the court to pay restitution. However, this process may take a long time, and it is rarely possible to associate any restitution paid with a specific refund fraud incident because these prosecutions generally involve more than fraudulent refund schemes. Officials also noted that in cases that do not result in criminal prosecutions, IRS does not often recover the stolen refund.

⁷The number of refund fraud cases in table 3 is greater than the number of cases listed in tables 1 and 2 because the earlier tables list cases where the identity of the legitimate taxpayer had been determined. Table 3 includes cases where IRS was in the process of making those determinations.

IRS Has Implemented New Initiatives in an Effort to Detect and Resolve Identity Theft Cases, but Not Enough Is Known about How Well the Initiatives Are Working

In 2008 and 2009, IRS implemented four initiatives to detect and resolve identity theft cases: identity theft account indicators, screening procedures for returns with indicators, the Identity Protection Specialized Unit (IPSU), and call centers with an identity theft telephone hotline.

Identity Theft Indicators Placed on Taxpayer Accounts

In January 2008, IRS began placing identity theft indicators, Transaction Code (TC) 971, on taxpayers' accounts where IRS determined there to be current or potential identity theft issues. The indicators are visible to all IRS personnel with account access. The purpose is to help both IRS and the taxpayer by making sure all IRS activities know that the taxpayer is an identity theft victim so that the taxpayer does not have to repeatedly explain this or prove his or her identity. The indicator also will alert IRS personnel that a future account problem may be the result of a previous identity theft incident; IRS expects this to help expedite future problem resolution.

In tax year 2008, IRS detected incidents of identity theft and placed indicators on those taxpayer accounts, as shown in table 4. The TC 971 is shown by one of four indicators that indicate taxpayers are victims of identity theft. The indicator used by IRS depends on the circumstances in which IRS receives indication of an identity theft-related problem.⁸

⁸ IRS intends to develop additional indicators for the 2010 filing season, including indicators for SSN-related and employment fraud problems.

Table 4: Numbers of Incidents and Taxpayers with Identity Theft-Related Indicators Cataloged as of December 31, 2008 (encompassing multiple tax years for 501 and 506 indicators)

Action code	Definition of indicator	Number of incidents	Number of taxpayers affected
501	Taxpayer receives indications from IRS activity about potential problems on their account and the taxpayer believes they may be a victim of identity theft	33,866 ^a	24,182
504	Taxpayer's identify information is stolen (the theft does not involve IRS), but taxpayer notifies IRS as a precaution	^b	643 ^c
505	IRS loses taxpayer data, which may result in identity theft-related issues for the taxpayer	149	911
506	IRS determines that a taxpayer is a victim of identity theft through review of taxpayer account and return	17,836 ^a	16,696

Source: GAO analysis of IRS data.

^aThe number of incidents of identity theft is higher than the number of taxpayers because a taxpayer can have more than one incident of identity theft.

^bThe number of incidents was not available.

^cOnly 3 months of data are provided because IPSU was not established until October 2008.

Once IRS substantiates the identity theft and the identity of the innocent taxpayer,⁹ either through IRS processes or the taxpayer providing documentation of the identity theft, IRS will place the indicator on the taxpayer's account and will notify the taxpayer.¹⁰ In the case of the 501 or 504 indicators, if the taxpayer does not substantiate the identity theft, IRS will not place the indicator on the taxpayer's account. IRS processes do not require substantiation for a 505 or 506 indicator because, in those cases, IRS independently determines the taxpayer's identity. IRS will remove an indicator after 3 consecutive years if there are no incidents on the account or will remove an indicator sooner if the taxpayer requests it.

Screening 2009 Returns for Possible Identity Theft-Related Refund Fraud

During the 2009 filing season, IRS screened returns filed in the names of taxpayers with 501 and 506 indicators looking for characteristics indicating that a return was filed by an identity thief instead of the legitimate taxpayer. IRS did not run the 504 and 505 indicators through the screening procedures in 2009. IRS officials told us in August 2009 that they plan to use the results of the 2009 screening as they consider whether to expand the screening to include 504 and 505 indicators in the 2010 filing

⁹Substantiation documentation includes copies of photo identification and a police report or an FTC identity theft affidavit.

¹⁰More information about which IRS activities assign which action codes can be found in table 6 in app. II.

season. The purpose of the screening was to prevent false returns from posting and to allow legitimate returns to quickly be placed back in regular return processing. Identity theft subject matter experts created the screen based on patterns they identified as being typical of identity thieves attempting to fraudulently gain refunds. If a return failed the screening, it was subject to additional reviews by IRS personnel. (See fig. 4 in app. III for a graphical representation of this process).

From January 2009 through June 2009, 18,183 returns had not passed the screening procedures; as of July 2009, 2,503 of these returns were still being analyzed to determine which were legitimate and which were filed by identity thieves.

Identity Protection Specialized Unit

In October 2008, IRS established IPSU to serve as a central point of contact primarily for taxpayers who had their identity stolen and wanted to notify IRS as a precaution before they had tax-related identity theft problems. IPSU processes these taxpayers' substantiation documentation and places a 504 indicator on their accounts.

In some cases, taxpayers contact the IPSU after another IRS activity has already identified an identity theft issue, or the taxpayer may send his or her identity theft substantiation documentation to the IPSU instead of the IRS activity responsible for resolving the problem. IPSU forwards such information to the correct IRS activity and monitors the taxpayer's account to see if the other activity substantiates the identity theft, places a 501 indicator on the account, and resolves identity theft-related issues. From October 2008 through June 2009, IPSU monitored 19,910 cases with tax-related identity theft issues.

IPSU does not monitor accounts where the taxpayer deals directly with another IRS activity unless contacted by the taxpayer. Nor does IPSU resolve taxpayers' identity theft-related issues. Problem resolution responsibility stays with the IRS activity where the problem originated. IRS officials concluded that it would slow down resolution of taxpayer issues and require more staff time to transfer problems from the activity that found the problem to IPSU for resolution.

Call Centers Supporting a
Dedicated Identity Theft
Hotline

Based on a recommendation from TAS,¹¹ IPSU sampled a small number of identity theft cases with the 501 indicator to look for evidence of identity theft-related problems that neither IRS nor the taxpayer have identified. For each sampled case, IPSU looked across the taxpayer's account and found a majority of these accounts had other identity theft issues. Subsequently, IPSU retroactively reviewed all cases with a 501 indicator. Based on this assessment, IPSU will take on an additional role starting in August 2009 by doing a similar review of all cases where a 501 indicator was placed on an account. If IPSU identifies a new identity-theft related issue on an account that they cannot resolve, IPSU will forward the information to the proper IRS activity to resolve.

Taxpayers who know of or suspect identity theft can call a dedicated toll-free number, established in October 2008, where customer service representatives can review his or her information and account history, answer questions, and explain what documentation is needed to substantiate the identity theft. From October 2008 through June 2009, the specialized call centers received 87,138 calls and provided service to 82,470 taxpayers. These numbers do not include identity theft-related calls received on IRS's general toll-free number.

IRS Implemented Its
Identity Theft Initiatives
Without Measures to
Assess How Well They Are
Working

IRS has not assessed the value of its new initiatives. IRS officials said they want to make such assessments. However, currently IRS has not defined measures that would provide an empirical basis for answering questions such as those listed below. This list of questions is not meant to be exhaustive.

- How many false positives (cases where a legitimate return is flagged as being fraudulent) and false negatives (cases where a fraudulent return is not flagged) are generated by the screening process?
- How long does it take and what is the cost to resolve cases that do not pass the screening and get reviewed by IRS personnel? This is important to taxpayers because refunds are held up while the review is conducted.
- How well does the current division of responsibility for resolving identity theft cases work or would a more centralized process work better?

¹¹National Taxpayer Advocate, *2008 Annual Report to Congress* (Washington, D.C: Dec 31, 2008).

-
- How well are taxpayers' questions answered and issues resolved using the hotline?¹²

IRS has developed objectives for its Identity Protection Strategy, which is a step towards effective performance measurement:

- reduce taxpayer burden while addressing and resolving identity theft cases,
- protect Treasury revenue by identifying suspicious filings before the refunds are generated, and
- increase operational efficiency of IRS by detecting and processing reported identity theft incidents as early and consistently as possible.

Further, PIPDS has recently developed one identity theft-related performance measure, "Increase revenue protected from erroneous refunds to identity thieves" and is reviewing the results of returns that were run through the business rules to capture data for this measure. PIPDS also stated that it has contracted with a consultant to help develop a suite of performance measures by the end of 2009. However, at the time we concluded our work, it was not known whether the performance measures will answer the types of questions we outlined above. Furthermore, for the measures to be in place in time to assess the initiatives performance during the 2010 filing season, timely action will be required. The measures will need to be developed early enough to give IRS time to develop a plan for capturing the data needed to implement the measures.

The answers to questions such as those listed above were not available when IRS designed its identity theft initiatives. IRS did not have an empirical basis for knowing what approach, such as having IRS activities rather than IPSU resolve cases, would work best. Furthermore, there have been some glitches with implementation. PIPDS officials told us that they are aware that some IRS activities have not been consistent in how they applied the identity theft indicators, causing some discrepancies in how returns were run through the screening procedures. For example, some activities would put the indicator on the taxpayer's account before ensuring that the information by the identity thief was removed from the taxpayer's account. Therefore, this resulted in legitimate taxpayer's returns failing the business rule screening and may have delayed the

¹² IRS officials told us that they have not received any negative feedback from taxpayers; however, they have not specifically asked for feedback, for example, through surveys.

taxpayer's refund. In June 2009, PIPDS officials subsequently met with the different IRS activities to revise their procedures for placing indicators on taxpayer accounts before the 2010 filing season.

Our own review of the effectiveness of the identity theft indicator and screening process also uncovered some possible issues. We compared IRS data from PIPDS and CI to test whether IRS issued refunds to suspected identity thieves in cases where there was already a 501 or 506 identity theft indicator on the account of the innocent taxpayer. We used the limited data available for 2009 because we wanted to look at cases handled after the new initiatives were put in place. As shown in table 5, we found that IRS failed to prevent a fraudulent refund 15 times in early 2009 even though the account had an identity theft indicator. During the same period, CI stopped 3,281 refunds, 14 percent of which had an identity theft indicator on the associated taxpayer account. Our analysis covers only part of the year and the initiatives are still new, so it is not possible to know whether this represents the long-term effectiveness of the initiative or not.

Table 5: Percentage of Suspected Identity Theft Refunds Stopped and Issued by IRS When Indicators Were on the Taxpayers' Accounts, Partial Calendar Year 2009

	Refund stopped	Refund issued
Number of returns	3,281	559
Number of returns with indicators	474	15
Percentage of returns with indicators	14	3

Source: GAO analysis of IRS data.

Note: The data used in this analysis are from January 1, 2009, through April 30, 2009. IRS identifies many refund fraud cases after the filing season is over, so this figure represents only a portion of the cases that will likely be identified in 2009.

Further, according to TAS officials, the number of TAS cases that involved identity theft issues in the first half of fiscal year 2009 was more than twice as high as it was in the same period in fiscal year 2008. Based on analyzing Taxpayer Advocate data, 8,880 taxpayers for whom TAS opened cases with identity theft issues in the first half of fiscal year 2009, 943 (about 11 percent) contacted TAS on their own initiative after another IRS activity had already placed a 501 or 506 indicator on their accounts. The presence of the indicator means that IRS was already working to resolve the taxpayer's tax problems before the taxpayer contacted TAS. As with our analysis of the screening process, these results need to be interpreted with caution. TAS policy is to always note identity theft problems in the TAS database, even when the taxpayer contacted TAS about a different

problem. In addition, because the indicators were so new we cannot be sure that the TAS data reflect their long-term effects. Also, some of the communication with taxpayers about their identity theft issues included TAS contact information, and PIPDS officials noted that some taxpayers may have contacted TAS thinking that it was the IRS office to which they should direct their questions.

Our analysis of screening program results and TAS data suggests that IRS's identity theft initiatives could be having a positive effect, but the evidence is not at all conclusive. The results do show that the initiatives have had some glitches; for example, some fraudulent refund payments were made despite the presence of an indicator. Overall, our analysis highlights the importance of IRS developing performance measures that will provide a basis for monitoring the effectiveness of the initiatives over time.

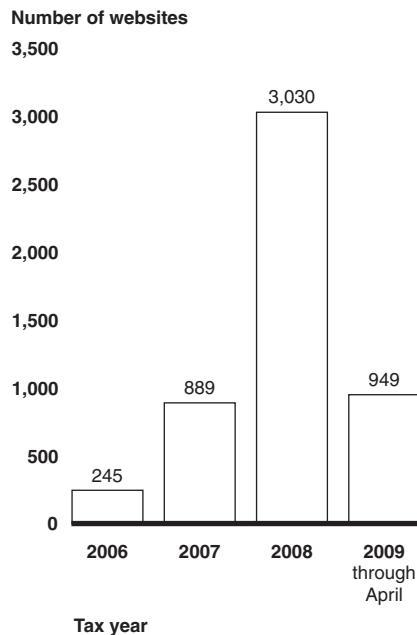
IRS Processes to Prevent Identity Theft through Phishing or Security Breaches

IRS provides taxpayers with targeted information to increase their awareness of identity theft, tips and suggestions for safeguarding taxpayers' personal information, and information to help them better understand tax administration issues related to identity theft. A new segment of the IRS home page, www.irs.gov, provides taxpayers with identity theft information including emerging trends, phishing sites, fraud schemes, and prevention strategies. According to IRS officials, they receive information on potential phishing schemes primarily from citizens sending IRS the information via phishing@irs.gov. These officials said IRS is directing victims to the most up-to-date identity theft information to ensure that they know how to report identity theft crimes and have the necessary resources and support to recover their identities. Additionally, IRS has worked to revise its most widely used documents, such as Form 1040, to include information about identity theft. To raise awareness with paid preparers, IRS officials are making identity theft and phishing presentations at the annual nationwide tax forums held for preparers.

In 2007, IRS created the Online Fraud Detection and Prevention (OFDP) office to reduce online fraud against IRS and taxpayers and provide a rapid response capability to detect and respond to such fraud. OFDP relies on tips from the public sent to phishing@irs.gov and other information sources. Once a fake electronic filing site is found, the team gathers information, such as screen shots of the site, and then passes it to CI and TIGTA for investigation. IRS sends a taxpayer identified as a possible victim a notification letter and a request asking the taxpayer to report the incident to FTC, contact the fraud departments of major credit bureaus, close any accounts that have been tampered with, and contact IPSU for

further information. Additionally, officials stated that OFDP is currently investigating processes to securely transmit compromised credit card information to banks. In addition, OFDP contacts the Web site's hosting provider to notify them that one of their customers is hosting a phishing site, and asks the hosting provider to voluntarily take down the site or remove the fraudulent content. According to the OFDP Director, the number of fraudulent Web sites taken down increased to 3,030 in 2008, as shown in figure 3.

Figure 3: Number of Fraudulent Web Sites Taken Down, 2006-2009



Source: GAO analysis of IRS data.

IRS faces challenges combating fraudulent Web sites. OFDP officials stated that schemes and Web sites that originate outside the United States are particularly challenging because of jurisdictional issues. However, the officials also said that IRS is working with TIGTA,¹³ DOJ, and other organizations to use existing authorities and relationships to assist with combating such fraud. Another challenge is the ability of fraudulent

¹³TIGTA audits and investigates IRS's operations to (1) promote economy and efficiency and detect and prevent fraud and abuse and (2) recommend actions for improvement.

IRS Information Security Weaknesses

parties to use multiple computer IP addresses that change frequently, making it difficult to trace the perpetrator's actual IP address. Finally, according to officials, some institutions are reluctant to share specific information about online fraud perpetrated against them. To help overcome this, officials stated that they are working with organizations such as the National Cyber Forensics and Training Alliance, Anti-Phishing Working Group, and others, to facilitate and improve information sharing about fraud schemes.

IRS has considered additional steps to help combat phishing and similar identity theft schemes such as providing a list of legitimate Web sites. However, such a list would be almost impossible to keep current.

Although IRS does not know of any cases where information security weaknesses have led to actual identity theft, as was noted earlier in table 4 IRS had 149 incidents of lost data affecting 911 taxpayers in 2008. Perhaps more importantly, IRS has information security weaknesses that increase the likelihood of IRS employees committing identify theft.¹⁴ Specifically, in January 2009 we reported that IRS did not consistently implement controls that were intended to prevent, limit, and detect unauthorized access to its systems and information.¹⁵ We noted that IRS did not always (1) enforce strong password management for properly identifying and authenticating users and (2) authorize user access, including access to personally identifiable information, to permit only the access needed to perform job functions. For example, the agency allowed authenticated users on its network access to shared drives containing taxpayer information as well as performance appraisal information for IRS employees including their SSNs. We made recommendations to IRS regarding ways to strengthen its information security practices. IRS agreed with the recommendations and stated that the agency is working to improve its security posture, and will develop a detailed corrective action plan addressing each of our recommendations. Until IRS addresses these weaknesses, there is an increased risk that someone could use his or her access to steal personally identifiable information and commit identity theft-related crimes.

¹⁴GAO has not determined if an IRS employee has committed any identity theft as a result of these weaknesses.

¹⁵GAO, *Information Security: Continued Efforts Needed to Address Significant Weaknesses at IRS*, [GAO-09-136](#) (Washington, D.C.: Jan. 9, 2009).

Privacy and Other Laws Limit IRS's Coordination with Other Agencies on Identity Theft Cases

Section 6103 of the Internal Revenue Code (I.R.C.) limits the types of information IRS can share with external parties, including identity theft victims, employers who may have workers using stolen identity information, or other government agencies, including law enforcement agencies. Under section 6103, tax returns and other information submitted to and, in some cases, generated by, IRS, are confidential and protected from disclosure, except as specifically authorized by statute.

IRS can disclose identity theft-related events that occur on a taxpayer's account to the taxpayer, such as the fact that an unauthorized return was filed using the taxpayer's information or that the taxpayer's SSN was used on another return. However, IRS may only disclose to the taxpayer the taxpayer's own return information. Therefore, IRS cannot disclose any other information about a fictitious Form 1040 or an incorrect Form W-2 submitted to IRS, or any information about IRS's investigation into the civil or criminal tax liability of the perpetrator (whether refund fraud or employment fraud) to the victim. In addition, IRS cannot disclose information about the perpetrator's identity to the taxpayer.

IRS can notify an employer whose employee has used a stolen SSN that the SSN on the Form W-2 filed for that employee does not belong to that individual. IRS can disclose to the employer that there is a mismatch between name and SSN and that the number belongs to someone else. However, IRS cannot disclose any further information such as the identity of the true owner of the SSN, to the employer. The employer is required to file a Form W-2 with accurate information and to file a corrected form if necessary. If an employer fails to file information returns or fails to include complete and correct information on them, IRS is authorized to penalize the employer. However, in prior work, we have reported that because of limited requirements for employers to verify and report accurate employee names and SSNs, few, if any, employers are likely to be penalized.¹⁶ For example, if employers establish reasonable cause for the incorrect Form W-2 information by showing they solicited an SSN from each employee one to three times, depending on the circumstances, and

¹⁶GAO, *Tax Administration: IRS Needs to Consider Options for Revising Regulations to Increase the Accuracy of Social Security Numbers on Wage Statements*, [GAO-04-712](#) (Washington, D.C.: Aug., 31, 2004).

that they used this information to complete the wage statements, IRS will waive the penalties on the employers.¹⁷

In 2008, IRS carried out a servicewide analysis of its efforts related to notification of identity theft victims and employers and information sharing with other federal agencies. IRS sought to determine if it was fully utilizing its disclosure authority under section 6103 to address the problem of identity theft and assist victims. The working group conducting the analysis determined that IRS was appropriately using its disclosure authority, though it also identified a few areas where IRS had authority to expand victim/employer notification and information sharing with federal law enforcement, if doing so was deemed sound policy. IRS is in the planning phase of an initiative to notify victims of employment fraud.

Section 6103 also limits the types of information indicating identity theft that the IRS can share with other agencies. For example, according to officials in IRS's Office of Chief Counsel, IRS can only share limited information about employment fraud with the Department of Homeland Security (DHS) and the Social Security Administration (SSA). A circumstance where IRS can share some information with federal law enforcement/immigration agencies is when IRS performs a criminal investigation. In these cases IRS can make investigative disclosures, i.e., the sharing of specific, limited information necessary for receiving information from other agencies that might support or further IRS's investigation. Disclosure of taxpayer information to state and local law enforcement agencies is even more limited. As mentioned previously, officials stated that IRS is currently investigating processes to securely transmit compromised credit card information to banks.

IRS officials also noted that tax fraud is not one of the 11 felony offenses enumerated in 18 U.S.C. §1028A, the Aggravated Identity Theft Statute. This means that in federal identity theft prosecutions, identity thieves would not be subject to the enhanced sentencing prescribed in the statute, an additional 2-year term of imprisonment. They also stated that this may be one factor that deters other federal law enforcement agencies and federal prosecutors from referring identity theft cases to IRS to look for

¹⁷Under Treas. Reg. § 301.6724-1; Publication 1586, *Reasonable Cause Regulations and Requirements for Missing and Incorrect Name/TINs*, establishing reasonable cause consists of making an initial request for the employee's name and SSN and, depending upon the circumstances, an annual solicitation thereafter. Employers must then show they have used this solicited information when submitting the information return(s) in question.

possible tax fraud or making identity theft-related tax fraud a priority when determining which cases to pursue.

According to PIPDS officials, activities that place 501 and 504 indicators on taxpayer accounts do not routinely accept information about identity theft victims from other federal agencies or other external parties. IRS does not routinely accept this information because it does not meet IRS's substantiation requirements.

Section 6103 does not limit IRS's ability to share more general information about how to manage identity theft. PIPDS has coordinated with private industry leaders, tax professionals, and other federal agencies on identity theft prevention, detection, and taxpayer assistance about how to handle tax-related identity theft issues and to share information about the increase in online fraud threats. PIPDS officials also meet with officials from other federal agencies such as SSA, FTC, and DHS and held a forum in July 2008 to share information on the effects of identity theft on victims and to identify best practices for preventing and resolving identity theft issues. According to PIPDS, one result of the forum was that IRS co-sponsored, along with the FTC, DHS, US Postal Inspection Service, Department of Commerce, DOJ, and the Securities and Exchange Commission, an educational website, www.onguardonline.gov. IRS is also coordinating with agencies to shut down phishing sites and online fraud schemes. According to CI and PIPDS, they are members of the Identity Theft Enforcement Interagency Working Group which shares information about leading identity theft activities, groups, and offenders with federal agencies that pursue identity theft cases.

Conclusion

While identity theft is known to cause tax problems for a relatively small number of taxpayers, for those affected the problems can be severe and include refunds frozen and time wasted. In an effort to more efficiently identify refund fraud and employment fraud as well as to assist innocent taxpayers, IRS put in place four new initiatives. Although IRS management has begun to develop performance measures, it is not known how well the measures will assess the effectiveness of the four initiatives.

Furthermore, it would be desirable to have the new measures in place for the 2010 filing season for at least two reasons. First, most refund fraud is committed during the filing season and also most employment fraud is detected as part of the filing process. Second, IRS is expanding the identity theft initiatives for the 2010 filing season. Without performance measures

in place, neither Congress nor IRS management will know whether the 2010 changes are effective or if additional changes are needed.

Recommendation for Executive Action

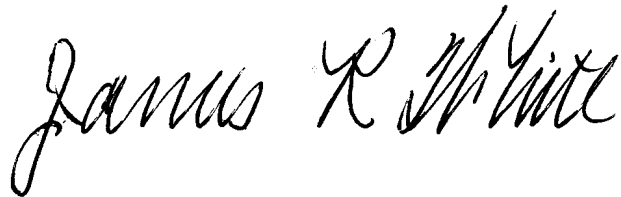
We recommend that the Commissioner of Internal Revenue ensure that performance measures suitable for assessing the effectiveness of its identity theft initiatives, and associated data collection procedures, are in place at the beginning of the 2010 filing season.

Agency Comments

The Commissioner of Internal Revenue provided written comments on a draft of this report in an August 31, 2009, letter, which is reprinted in appendix IV. The Commissioner agreed with our recommendation. In his letter, the Commissioner discussed IRS's commitment to reduce the impact of identity theft on taxpayers and said that he has made it a priority at IRS to reduce the burden placed on the taxpayer and the tax system because of identity theft. IRS provided separate comments on technical issues, which we incorporated into this report where appropriate.

As agreed with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from its issue date. At that time, we will send copies to the Secretary of the Treasury; the Commissioner of Internal Revenue, and other interested parties. This report will also be available at no charge on GAO's Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-9110 or whitej@gao.gov. Contact points for our offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix V.

A handwritten signature in black ink that reads "James R. White". The signature is written in a cursive style with a large, prominent initial "J".

James R. White
Director, Tax Issues
Strategic Issues Team

Appendix I: Objectives, Scope, and Methodology

The objectives of this report were to (1) describe how much identity theft-related refund and employment fraud the Internal Revenue Service (IRS) faces and whether incidents of identity theft go undetected by IRS, (2) assess the actions IRS is taking to prevent and detect identity theft-related tax problems and to assist affected taxpayers, and (3) describe what IRS is doing to coordinate its identity theft-related efforts with other government and nongovernment entities.

To understand how much identity theft-related refund and employment fraud IRS faces, we interviewed IRS officials from the Office of Privacy, Information Protection and Data Security (PIPDS), Wage and Investment Division (W&I), Small Business/Self-Employed Division (SB/SE), Criminal Investigation Division (CI), and Submission Processing. We discussed the processes and systems used to identify identity theft-related refund fraud and IRS's use of the identity theft indicators. Additionally, we analyzed information from PIPDS on the number and characteristics of identity theft-related refund and employment fraud by cases and affected taxpayers, including the activity reporting the incident and the type of identity theft indicator placed on the taxpayer account. Based on the information we collected on the identity theft-related incidents and affected taxpayers, we also were able to discuss the outcomes of the identity theft-related refund fraud cases and identify the reasons which incidents of identity theft go undetected.

To determine the reliability of the PIPDS data sets, we interviewed knowledgeable officials to discuss processes followed to upload the taxpayer data, collection methods, and the data reported on and for what purpose. We also reviewed related documentation to determine the accuracy of the 2008 year-end aggregate numbers of taxpayers affected and identity indicators placed on accounts. PIPDS provided us with monthly reports on the number of taxpayers affected and incidents reported as well as an annual report totaling these numbers. We compared the monthly reports to the aggregated data to identify any obvious errors in accuracy and completeness. We determined that the PIPDS data we used for this objective were sufficiently reliable for this assessment.

To assess what actions IRS is taking to prevent and detect identity theft-related problems and to assist affected taxpayers, we interviewed officials from PIPDS, W&I, SB/SE, CI, the Online Fraud Detection and Prevention office (OFDP), and the Taxpayer Advocate Service (TAS). We discussed new initiatives IRS has implemented to detect and resolve identity theft as well as assist affected taxpayers and educate taxpayers about identity theft. We also reviewed prior GAO work to obtain information on identity

theft-related issues in the federal government and on systems used to safeguard IRS data and to identify identity theft-related incidents, as well as Treasury Inspector General for Tax Administration (TIGTA) reports to obtain information on the identity theft-related processes and procedures used by IRS. Additionally, we collected and analyzed IRS's Identity Protection Strategy, policies and procedures related to identity theft prevention and detection and assistance, relevant sections of the Internal Revenue Manual and Internal Revenue Code, and governmentwide guidance on performance measures. To understand how IRS implemented some of the new initiatives, we visited the Andover, Massachusetts campus and reviewed processes followed by the Identity Protection Specialized Unit (IPSU) and the Baltimore call center to listen to calls taken by customer service representatives on the identity theft hotline. Additionally, we met with and reviewed the software used by the OFDP staff when taking down a fraudulent Web site. For these new initiatives, we collected data on the number of affected taxpayers whose records had identity theft indicators, the number of cases worked by the IPSU, information on calls received by the dedicated identity theft call-in number, and the number of fraudulent Web sites taken down by OFDP. We reviewed the data and documents provided by IRS in conjunction with discussions with IRS officials in order to describe these new initiatives as well as to understand the extent to which IRS had performance measures to determine the effectiveness of the new initiatives. We used previous GAO work and recommendations to describe systems and information security weaknesses and assessed how these weaknesses may translate to identity theft-related issues for IRS and taxpayers.

To assess whether IRS's initiatives were working as intended, we interviewed PIPDS and TAS officials and used IRS and TAS data to identify (1) the frequency with which suspected identity theft-related refund fraud reoccurred for taxpayers known to have had identity theft issues in the past and (2) how often taxpayers took identity theft-related tax problems to TAS after other IRS functions had determined that their issues were related to identity theft. To assess whether the business rules were working as intended, we tested suspected identity theft-related refunds that were identified by CI to determine how many of the corresponding taxpayers had indicators on their accounts before the refunds were stopped or issued by IRS. To perform this assessment we received from PIPDS taxpayer data on all taxpayer accounts that had indicators on them. We also received from CI taxpayer data on all suspected identity theft-related refunds that were identified, stopped, and issued by IRS from January 1, 2009, through April 30, 2009. To assess how often taxpayers took their issues to TAS after an identity theft indicator

had been placed on their accounts, we compared taxpayer data from TAS with identity theft as a primary or secondary issue code to data from PIPDS identifying all taxpayer accounts with identity theft indicators. We compared the dates the identity theft indicator was placed on the accounts to the dates when TAS received the cases. Additionally, we reviewed the reason why the cases came to TAS based on each identity theft indicator. We requested TAS cases received from October 1, 2008, through May 18, 2009, and PIPDS indicator data from calendar year 2008.

We received taxpayer data from PIPDS, CI, and TAS. To ensure the reliability of the data, we performed an analysis using Statistical Analysis Software (SAS) to test for obvious errors in accuracy and completeness. Additionally, we reviewed related reports to determine if there were any discrepancies in the data we received. Any questions we had about the data were answered by knowledgeable officials with whom we also discussed the processes followed to upload the taxpayer data, collection methods, and the data reported on and for what purpose. We determined that the PIPDS, CI, and TAS data we used for this analysis were sufficiently reliable to use for this assessment.

To identify what IRS is doing to coordinate its identity theft-related efforts with those of other government agencies and other entities as well as to identify any lessons learned, we interviewed officials from IRS's PIPDS, Office of General Counsel, OFDP, and W&I. We also reviewed documentation provided by IRS officials, a recorded version of the IRS identity protection forum held in July 2008, and previous GAO work. We also reviewed an IRS general counsel analysis and discussion of Section 6103 of the Internal Revenue Code to determine the circumstances in which IRS can share information with other federal agencies, law enforcement employers, and the taxpayers for identity theft-related refund and employment fraud issues.

We conducted this performance audit from October 2008 through August 2009 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Description of Indicator Codes Used to Identify Tax and Non-Tax Related Issues

In January 2008, the Internal Revenue Service (IRS) began using indicator codes to identify taxpayers with identity theft-related issues. How the identity theft-related issue comes to IRS and the type of incident will dictate the indicator that will be placed on taxpayers' accounts. Based on the incidents, IRS can require additional documentation to substantiate the identity theft and run certain flagged accounts through additional screenings in subsequent years. See table 6 for a more detailed description of the indicators.

Table 6: Indicator Codes Used by IRS to Flag Taxpayer Accounts for Tax- and Non-Tax-Related Identity Theft Issues

Indicator codes	501	504	505	506
Indication of identity theft	Taxpayer receives indication from IRS program about potential problems on his or her account and believes that he or she may be a victim of identity theft	Taxpayer's personal identifying information is stolen outside of IRS, but taxpayer wants to take precautionary measures on his or her account	IRS loses taxpayer's personal identifying information, which could potentially cause identity theft issues for the taxpayer in the future	CI determines that a taxpayer is a victim of identity theft based on review of taxpayer's account
Tax related/ Non-tax related	Tax related	Non-tax related	Non-tax related	Tax related
Required documentation from taxpayer	Substantiation of identity theft	Substantiation of identity theft	None	None
Business units placing indicator on the account	Primarily W&I, SB/SE, TAS, and PIPDS	W&I (through IPSU)	PIPDS	Primarily CI
Run through business rules	Yes	No	No	Yes
Assistance to taxpayer	Indicator will stay on taxpayer account for 3 years and account will go through additional screening procedures for 3 years	Indicator will stay on taxpayer account for 3 years	Indicator will stay on taxpayer account for 3 years and taxpayer can receive free credit monitoring, which includes insurance to cover damages resulting from identity theft	Indicator will stay on taxpayer account for 3 years and account will go through additional screening procedures for 3 years

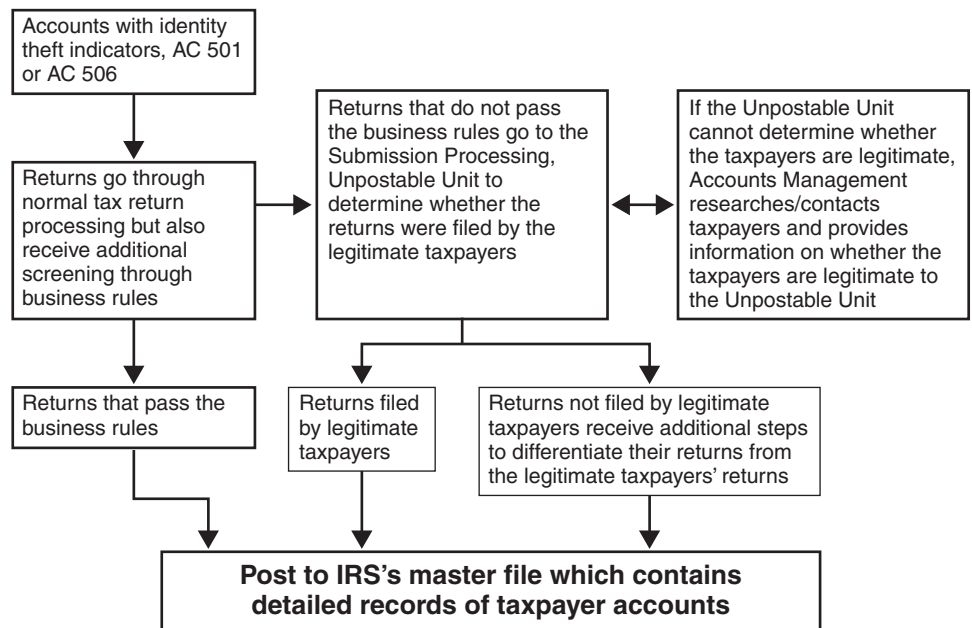
Source: GAO analysis of IRS information.

Appendix III: Procedures Followed for Additional Screening of Certain Indicator Accounts

Taxpayer accounts with a 501 or 506 indicator are run through additional screenings in subsequent years to determine the legitimacy of the return filed. The Internal Revenue Service (IRS) initially decided to run the 501 and 506 indicators through additional screenings because IRS processes determined those accounts to have identity theft directly impacting IRS.

Returns that pass the additional screening are sent through for regular processing. If a return fails the screening, the Unpostable Unit in Submission Processing will attempt to determine if the return was filed by the legitimate taxpayer or an identity thief. If the Unpostable Unit cannot resolve the problem, Accounts Management will conduct a more detailed analysis, which may include contacting the taxpayer. Once Accounts Management determines the owner of the return, they will forward the information back to the Unpostable Unit who will send the legitimate returns through for regular processing and mark any returns filed by identity thieves as bad.

Figure 4: Process Followed to Run Tax-Related Accounts with Indicator Codes through Additional Screening Procedures



Source: GAO analysis of IRS information.

Appendix IV: Comments from the Internal Revenue Service



COMMISSIONER

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

August 31, 2009

Mr. James R. White
Director, Tax Issues
Strategic Issues Team
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. White:

Thank you for the opportunity to comment on the draft report, *Tax Administration: IRS Has Implemented Initiatives to Prevent, Detect, and Resolve Identity Theft-Related Problems, but Needs to Assess Their Effectiveness* (Government Accountability Office-09-882). We appreciate that your draft report recognizes the progress that the Internal Revenue Service has made to prevent and detect identity theft-related problems and to assist affected taxpayers.

The security and privacy of taxpayer information is of the utmost importance to the IRS. We are committed to reduce the impact of identity theft on taxpayers. I have made it a priority of this agency to reduce the burden placed on the taxpayer and the tax system because of identity theft.

We appreciate GAO's continued work and focus on this issue. I agree that strong performance measures are critical for the long-term success of the program and the IRS will have them in place for the 2010 filing season.

If you have any questions or would like to discuss our response further, please contact Deborah Wolf, Director, Privacy, Information Protection and Data Security, at (609) 278-7732.

Sincerely,

A handwritten signature in black ink, appearing to read "D. Shulman".

Douglas H. Shulman

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

James R. White, (202) 512-9110 or whitej@gao.gov

Acknowledgments

In addition to the individual named above, David Lewis, Assistant Director; Sabine Paul, Assistant Director; Mary Fike; Suzanne Heimbach; Sairah Ijaz; Laurie King; Sabrina Streagle; and James Ungvarsky made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

