United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Government Organization, Efficiency and Financial Management, Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 12:30 p.m. EDT
Thursday, June 2, 2011

TAXES AND IDENTITY THEFT

Status of IRS Initiatives to Help Victimized Taxpayers

Statement of James R. White, Director
Strategic Issues

GAO
Accountability • Integrity • Reliability

Highlights

Highlights of GAO-11-721T, testimony before the Subcommittee on Government Organization, Efficiency and Financial Management, Committee on Oversight and Government Reform, House of Representatives

June 2, 2011

TAXES AND IDENTITY THEFT

Status of IRS Initiatives to Help Victimized Taxpayers

Why GAO Did This Study

Identity theft is a serious and growing problem in the United States. Taxpayers are harmed when identity thieves file fraudulent tax documents using stolen names and Social Security numbers. In 2010 alone, the Internal Revenue Service (IRS) identified over 245,000 identity theft incidents that affected the tax system. The hundreds of thousands of taxpayers with tax problems caused by identity theft represent a small percentage of the expected 140 million individual returns filed, but for those affected, the problems can be quite serious.

GAO was asked to describe, among other things, (1) when IRS detects identity theft based refund and employment fraud, (2) the steps IRS has taken to resolve, detect, and prevent innocent taxpayers' identity theft related problems, and (3) constraints that hinder IRS's ability to address these issues.

GAO's testimony is based on its previous work on identity theft. GAO updated its analysis by examining data on identity theft cases and interviewing IRS officials.

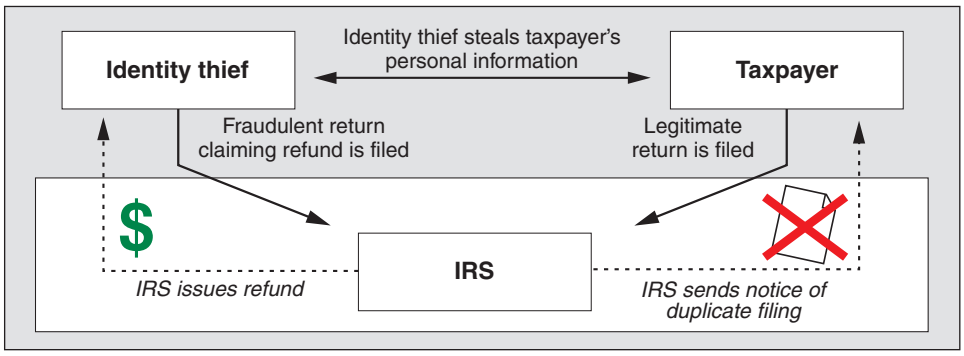
GAO makes no new recommendations but reports on IRS's efforts to address GAO's earlier recommendation that IRS develop performance measures and collect data suitable for assessing the effectiveness of its identity theft initiatives. IRS agreed with and implemented GAO's earlier recommendation.

View GAO-11-721T or key components. For more information, contact James R. White at (202) 512-9110 or whitej@gao.gov.

What GAO Found

Identity theft harms innocent taxpayers through employment and refund fraud. In refund fraud, an identity thief uses a taxpayer's name and Social Security Number (SSN) to file for a tax refund, which IRS discovers after the legitimate taxpayer files.

Notional Example of Refund Fraud



Source: GAO.

In employment fraud, an identity thief uses a taxpayer's name and SSN to obtain a job. When the thief's employer reports income to IRS, the taxpayer appears to have unreported income on his or her return, leading to enforcement action.

IRS has taken multiple steps to resolve, detect, and prevent employment and refund fraud:

Resolve—IRS marks taxpayer accounts to alert its personnel of a taxpayer's identity theft. The purpose is to expedite resolution of existing problems and alert personnel to potential future account problems.

Detect—IRS screens tax returns filed in the names of known refund and employment fraud victims.

Prevent—IRS provides taxpayers with information to increase their awareness of identity theft, including tips for safeguarding personal information. IRS has also started providing identity theft victims with a personal identification number to help identify legitimate returns.

IRS's ability to address identity theft issues is constrained by

- privacy laws that limit IRS's ability to share identity theft information with other agencies;
- the timing of fraud detection—more than a year may have passed since the original fraud occurred;
- the resources necessary to pursue the large volume of potential criminal refund and employment fraud cases; and
- the burden that stricter screening would likely cause taxpayers and employers since more legitimate returns would fail such screening.

Chairman Platts, Ranking Member Towns, and Members of the Subcommittee:

I am pleased to be here to discuss how identity theft harms taxpayers and how the Internal Revenue Service (IRS) works to resolve, detect, and prevent these problems. 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. Within the tax system, 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 identifying information. Taxpayers may also become subject to IRS enforcement actions after someone else uses the identity theft victim's identity to fraudulently obtain employment and the thief's income is reported to IRS by an employer in the victim's name. In 2010 alone, IRS identified over 245,000 identity theft incidents that affected the tax system. The hundreds of thousands of taxpayers with tax problems caused by identity theft represent a small percentage of the expected 140 million individual returns filed, but for those affected, the problems can be quite serious.

My testimony today will cover (1) when IRS detects identity theft-based refund and employment fraud, (2) the steps IRS has taken to resolve, detect, and prevent innocent taxpayers' identity theft-related problems, (3) constraints that hinder IRS's ability to address these issues, and (4) the potential for more rigorous screening to prevent refund or employment fraud now and in the future. My testimony is based on our previous 2009 and 2011 reports.[1] IRS agreed with and implemented our recommendation in our 2009 identity theft report to develop performance measures and collect data suitable for assessing the effectiveness of its identity theft initiatives. We updated our analysis with current data on identity theft cases and interviewed IRS officials in the Office of Privacy, Information Protection and Data Security (PIPDS). To determine the reliability of IRS data on identity theft, we discussed data quality-control procedures with agency officials, reviewed relevant documentation, and tested data for obvious errors. We determined that the data were sufficiently reliable for the purposes of this report.

[1]GAO, *Tax Administration: IRS Has Implemented Initiatives to Prevent, Detect, and Resolve Identity Theft-Related Problems, but Needs to Assess Their Effectiveness*, GAO-09-882 (Washington, D.C.: Sept. 8, 2009) and *Taxpayer Account Strategy: IRS Should Finish Defining Benefits and Improve Cost Estimates,* GAO-11-168 (Washington, D.C.: Mar. 24, 2011).

Our prior reports and this May 2011 update were conducted 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.

We discussed the new information in this statement with IRS officials, and they concurred with our findings.

IRS and Taxpayers May Not Discover Refund or Employment Fraud until after Legitimate Tax Returns Are Filed

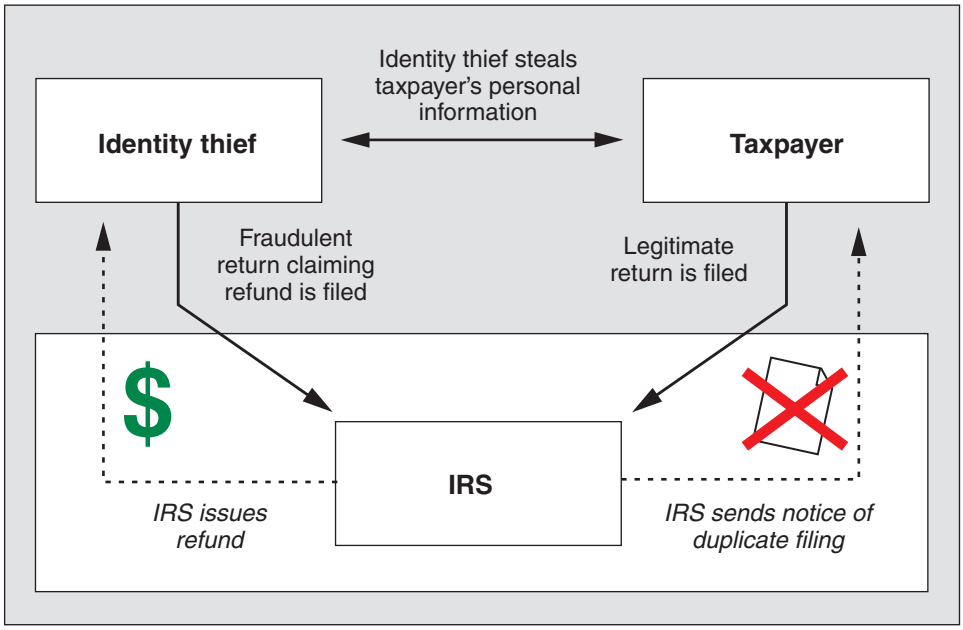
The number of tax-related identity theft incidents (primarily refund or employment fraud attempts) identified by IRS has grown:

- 51,702 incidents in 2008,
- 169,087 incidents in 2009, and
- 248,357 incidents in 2010.

Refund Fraud Delays Innocent Taxpayers' Refunds

Refund fraud can stem from identity theft when an identity thief uses a legitimate taxpayer's name and Social Security Number (SSN) to file a fraudulent tax return seeking a refund. In these cases, the identity thief typically files a return claiming a refund early in the filing season, before the legitimate taxpayer files. IRS will likely issue the refund to the identity thief after determining the name and SSN on the tax return appear valid (IRS checks all returns to see if filers' names and SSNs match before issuing refunds). IRS often first becomes aware of a problem after the legitimate taxpayer files a return. At that time, IRS discovers that two returns have been filed using the same name and SSN, as shown in figure 1. The legitimate taxpayer's refund is delayed while IRS spends time determining who is legitimate.

Figure 1: Notional Example of Refund Fraud

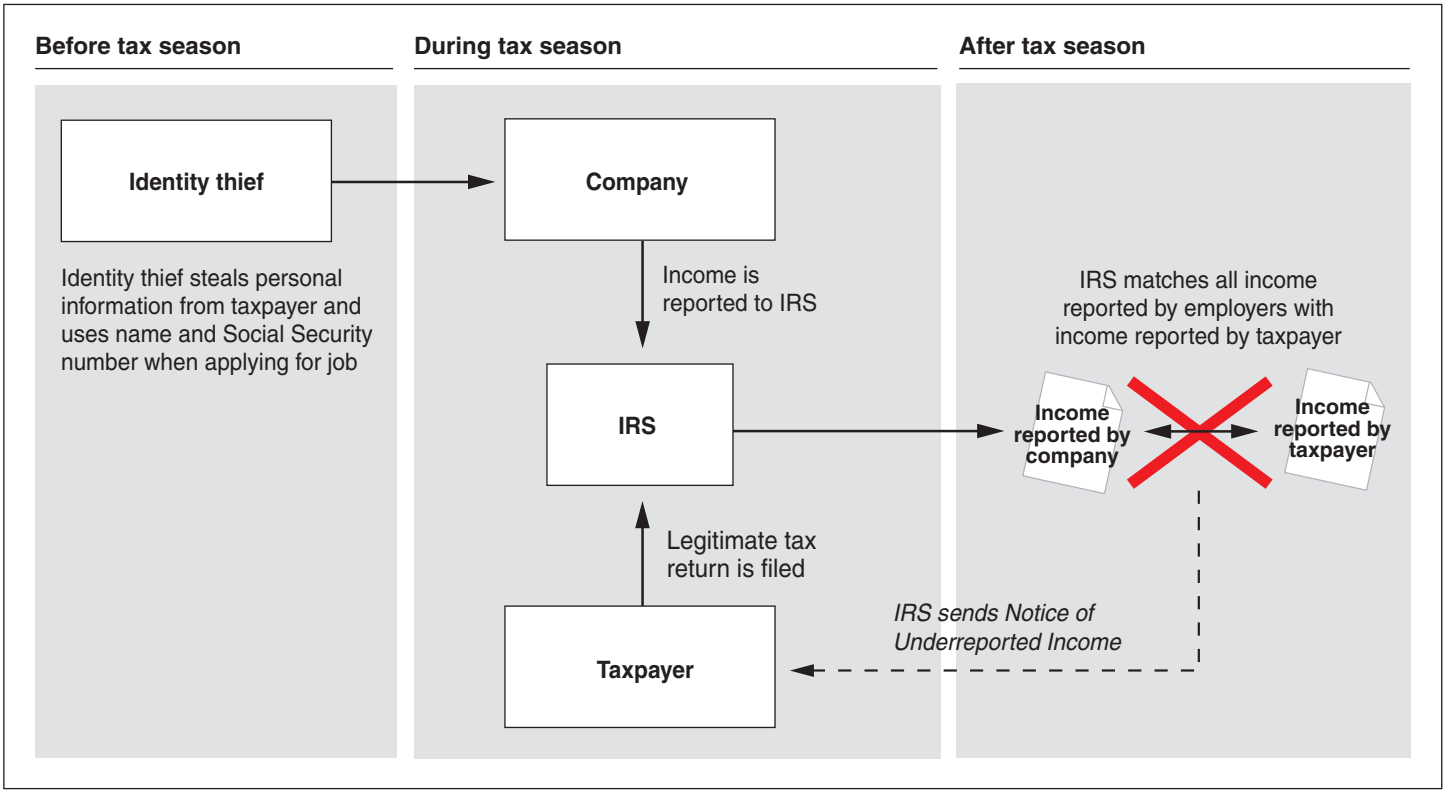


Source: GAO.

Employment Fraud Exposes Innocent Taxpayers to Enforcement Actions for Unreported Income

Employment fraud occurs when an identity thief uses a taxpayer's name and SSN to obtain a job. IRS subsequently receives income information from the identity thief's employer. After the victim files his or her tax return, IRS matches income reported by the victim's employer and the thief's employer to the tax return filed by the legitimate taxpayer, as shown in figure 2. IRS then notifies the taxpayer of unreported income because it appears the taxpayer earned more income than was reported on the tax return. Employment fraud causes tax administration problems because IRS has to sort out what income was earned by the legitimate taxpayer and what was earned by the identity thief.

Figure 2: Notional Example of Employment Fraud



Source: GAO.

To Date, Known Cases of Identity Theft Have Occurred outside IRS

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. IRS officials told us they are unaware of any incidents where information was stolen from IRS and used to commit employment or refund fraud. However, there are risks at IRS. In a recent audit, we found that although IRS has made progress in correcting previously reported information security weaknesses, it did not consistently implement controls intended to prevent, limit, and detect unauthorized access to its

systems and information, including sensitive taxpayer information.[2] In 2009, we also reported that third-party software used to prepare and file returns may pose risks to the security and privacy of taxpayer information.[3] IRS agreed with our recommendations to address these and other issues. We recently followed up with IRS on this issue and learned that IRS has begun monitoring adherence to security and privacy standards in the tax software industry.

IRS Has Taken Multiple Steps to Resolve, Detect, and Prevent Employment and Refund Fraud

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.

Indicators—account flags that are visible to all IRS personnel with account access—are a key tool IRS uses to resolve and detect identity theft. IRS uses different indicators depending on the circumstances in which IRS receives indication of an identity theft–related problem. Once IRS substantiates any taxpayer-reported information, either through IRS processes or the taxpayer providing documentation of the identity theft, IRS will place the appropriate indicator on the taxpayer's account and will notify the taxpayer. 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.

The three elements of IRS's strategy are resolution, detection, and prevention.

Resolution. Identity theft indicators speed resolution by making a taxpayer's identity theft problems visible to all IRS personnel with account access. Taxpayers benefit because they do not have to repeatedly explain their identity theft issues or prove their identity to multiple IRS units. Indicators also alert IRS personnel that a future account problem may be

[2]GAO, *Information Security: IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data*, GAO-11-308 (Washington, D.C.: Mar. 15, 2011). We made recommendations for corrective action, and IRS agreed to develop a detailed corrective action plan to address each recommendation.

[3]GAO, *Tax Administration: Many Taxpayers Rely on Tax Software and IRS Needs to Assess Associated Risks,* GAO-09-297, (Washington, D.C.: Feb. 25, 2009).

related to identity theft and help speed up the resolution of any such problems.

Since our 2009 report, IRS developed a new, temporary indicator to alert all IRS units that an identity theft incident has been reported but not yet resolved. IRS officials told us that they identified a need for the new indicator based on their ongoing evaluation of their identity theft initiatives. The temporary indicator's purpose is to expedite problem resolution and avoid taxpayers having to explain their identity theft issues to multiple IRS units.

As discussed in our 2009 report, taxpayers with known or suspected identity theft issues can receive assistance by contacting the Identity Protection Specialized Unit.[4] The unit operates a toll-free number taxpayers can call to receive assistance in resolving identity theft issues.

Detection. IRS also uses its identity theft indicators to screen tax returns filed in the names of known refund and employment fraud victims. During the 2009, 2010, and 2011 filing seasons, IRS screened returns filed in the names of taxpayers with identity theft indicators on their accounts. There are approximately 378,000 such taxpayers. In this screening, IRS looks for characteristics indicating that the return was filed by an identity thief instead of the legitimate taxpayer, such as large changes in income or a change of address. If a return fails the screening, it is subject to additional IRS manual review, including contacting employers to verify that the income reported on the tax return was legitimate. In addition to U.S. taxpayers with indicators on their accounts, IRS officials also told us that they screened returns filed in the name of a large number—about 350,000—of Puerto Rican citizens who have had their U.S. SSNs compromised in a major identity theft scheme.[5]

As of May 12, 2011, 216,000 returns filed in 2011 failed the screens and were assigned for manual processing. Of these, IRS has completed processing 195,815 and found that 145,537 (74.3 percent) were fraudulent.

[4]GAO-09-882.

[5]The number of accounts with indicators is not the same as the number of returns that are screened. A single taxpayer account, for example could be subject to many refund fraud attempts.

In January 2011, IRS launched a pilot program for tax year 2010 returns (due by April 15, 2011) using a new indicator to "lock" SSNs of deceased taxpayers.[6] If a locked SSN is included on a tax return, the new indicator will prompt IRS to automatically reject the return. PIPDS officials told us they intend to expand the pilot to include more SSNs of deceased taxpayers after analyzing the results of the initial pilot.

A program IRS uses to identify various forms of refund fraud—including refund fraud resulting from identity theft—is the Questionable Refund Program. IRS established this program to screen tax returns to identify fraudulent returns, stop the payment of fraudulently claimed refunds, and, in some cases, refer fraudulent refund schemes to IRS's Criminal Investigation offices.

Prevention. As described in our 2009 report, IRS has an office dedicated to finding and stopping online tax fraud schemes.[7] IRS also 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. Appendix I summarizes information IRS and FTC provide to taxpayers to protect themselves against identity theft.

Since our 2009 report,[8] IRS began a pilot program providing some identity theft victims with a 6-digit Identity Protection Personal Identification Number (PIN) to place on their tax return. IRS officials told us they created the PIN based on their ongoing evaluation of their identity theft initiatives. When screening future years' returns for possible identity theft, IRS will exclude returns with a PIN, which will help avoid the possibility of a "false positive" and a delayed tax refund. IRS sent letters containing an identity theft PIN to 56,000 taxpayers in the 2011 filing season. IRS will provide taxpayers a new PIN each year for a period of 3 years following an identity theft.

[6]The pilot consists of 6,000 deceased taxpayers who died before 2009, but filed returns in 2009. IRS selected these taxpayers for the pilot because of the high probability the taxpayers' returns were fraudulent.

[7]GAO-09-882.

[8]GAO-09-882.

IRS's Ability to Address Identity Theft Issues Is Constrained by Law, Timing, and Resources

Privacy and Other Laws Limit IRS's Coordination with Other Agencies and Taxpayers

IRS's initiatives to address identity theft are limited in part because 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.[9] As discussed in more detail in our 2009 report, 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 cannot disclose to the taxpayer any other information pertaining to employment or refund fraud, such as the perpetrator's identity or any information about the perpetrator's employer. Additionally, IRS has limited authorities to share identity theft information with other federal agencies. When performing a criminal investigation, IRS can make only investigative disclosures, that is, the sharing of specific, limited information necessary for receiving information from other federal agencies that might support or further IRS's investigation. Disclosure of taxpayer information to state and local law enforcement agencies is even more limited.

IRS Is Often Unable to Detect Suspicious Cases until after the Fraud Has Occurred

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 employment fraud until after the following year's tax filing deadline of April 15 when it matches income reported by employers against taxpayers' filed returns. It is only after IRS notifies a taxpayer of unreported income that IRS may learn from the taxpayer that the income was not the taxpayer's 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.

[9]Section 6103 of Internal Revenue Code.

IRS Does Not Pursue Criminal Investigations in Every Case of Potential Refund and Employment Fraud because of Resource Priorities

IRS officials told us that IRS pursues criminal investigations of suspected identity thieves in only a small number of cases. IRS's Criminal Investigations (CI) Division's investigative priorities include tax crimes, such as underreporting income from legal sources; illegal source financial crimes; narcotics-related financial crimes; and counterterrorism financing. In fiscal year 2010, CI initiated 4,706 investigations of all types, a number far smaller than the total number of identity theft–related refund and employment fraud cases identified in that year.

Also, the decision to prosecute identity thieves does not rest with IRS. CI conducts investigations and refers cases to the Department of Justice (DOJ), which is responsible for prosecuting cases in the federal courts. IRS officials said that the small number of tax-related identity theft cases that they investigate recognizes that DOJ has to conclude that the case is of sufficient severity that it should be pursued in the federal courts before it will be prosecuted. According to data from CI included in our prior report, the median amount of suspected identity theft–related refunds identified in the 2009 filing season was around $3,400.

CI has investigated tax-related identity theft cases that DOJ has successfully prosecuted. In our prior report we cited the example of a former Girl Scout troop leader serving 10 years in federal prison for stealing the SSNs of girls in her troop and then claiming more than $87,000 in fraudulent tax refunds.

Improved Detection of Employment and Refund Fraud Must Be Balanced against Burdens on Innocent Taxpayers and Costs

Options exist, now and in the future, to improve detection of identity theft–related tax fraud, but they come with trade-offs.

Known identity theft victims. IRS could screen returns filed in the names of known identity theft victims more tightly than is currently done. More restrictive screening may detect more cases of refund fraud before IRS issues refunds. However, more restrictive screening will likely increase the number of legitimate returns that fail the screenings (false positives). Since returns that fail screening require a manual review, this change could harm innocent taxpayers by causing delays in their refunds. Using more restrictive rules would also place additional burden on employers because IRS contacts employers listed on all returns that fail screening.

All taxpayers. Beyond screening returns with known tax-related identity theft issues, screening all tax returns for possible refund fraud would pose similar trade-offs, but on a grander scale. For example, as noted above,

one way to check for identity theft is to look for significant differences between current year and prior year tax returns, but this could be confounded by a large number of false positives. IRS officials told us that in 2009 there were 10 million address changes, 46 million changes in employer, and millions of deaths and births. Checking all returns that reflect these changes for possible refund fraud could overwhelm IRS's capacity to issue refunds to legitimate taxpayers in a timely manner.

Looking Forward. IRS's identity protection strategy and the creation of PIPDS were part of an effort to more efficiently identify refund and employment fraud as well as to assist innocent taxpayers. Since adopting the recommendation in our 2009 report regarding using performance measures to assess effectiveness,[10] IRS has followed through, using its improved performance information to identify additional steps it could take. These include the new indicators for taxpayer accounts, improved routing of suspect returns, and PIN numbers. However, none of these steps will completely eliminate refund or employment fraud. By continuing to monitor the effectiveness of its identity theft initiatives, IRS may find additional steps to reduce the problems faced by both taxpayers and IRS.

Looking further forward, other long-term initiatives underway at IRS have at least some potential to help combat identity theft–related fraud. In April 2011, the Commissioner of Internal Revenue gave a speech about a long-term vision to increase up-front compliance activities during returns processing. One example is to match information returns with tax returns before refunds are issued. Before this could happen, IRS would have to make significant changes. Third-party information returns would have to be filed with IRS earlier in the filing season.[11] IRS would also have to improve its automated processing systems; IRS's current Customer Account Data Engine (CADE 2) effort is one key step.[12] While these efforts are part of a broad compliance improvement vision, they could also detect some identity theft–related fraud. If, for example, IRS could match employer information to tax returns before refunds are issued, identity thieves could not use phony W-2s to claim fraudulent refunds.

[10]GAO-09-882.

[11]Many information returns, such as forms W-2 filed by employers, are not due to the government until the end of February.

[12]GAO-11-168.

Chairman Platts, Ranking Member Towns, and Members of the Subcommittee, this completes my prepared statement. I would be happy to respond to any questions you may have at this time.

Contacts and Acknowledgments

For further information on this testimony, please contact James R. White at (202) 512-9110 or whitej@gao.gov. In addition, contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. In addition to the individual named above, David Lewis, Assistant Director; Shannon Finnegan, analyst-in-charge; Michele Fejfar; Donna Miller; Erika Navarro; Melanie Papasian; and Sabrina Streagle made key contributions to this report.

Appendix I: Things Taxpayers Can Do to Protect Themselves if They Suspect Identity Theft

Both the Internal Revenue Service (IRS) and the Federal Trade Commission (FTC) provide helpful information to taxpayers to deter, detect, and defend against identity theft. 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. For example, IRS has published on its website the list in table 1 below.

Table 1: IRS's Top 10 Things Every Taxpayer Should Know about Identity Theft

1.	The IRS does not initiate contact with a taxpayer by e-mail.
2.	If you receive a scam e-mail claiming to be from the IRS, forward it to the IRS at phishing@irs.gov
3.	Identity thieves get your personal information by many different means, including: • Stealing your wallet or purse • Posing as someone who needs information about you through a phone call or e-mail • Looking through your trash for personal information • Accessing information you provide to an unsecured Internet site.
4.	If you discover a website that claims to be the IRS but does not begin with 'www.irs.gov', forward that link to the IRS at phishing@irs.gov
5.	To learn how to identify a secure website, visit the Federal Trade Commission at www.onguardonline.gov/tools/recognize-secure-site-using-ssl.aspx
6.	If your Social Security number is stolen, another individual may use it to get a job. That person's employer may report income earned by them to the IRS using your Social Security number, thus making it appear that you did not report all of your income on your tax return.
7.	Your identity may have been stolen if a letter from the IRS indicates more than one tax return was filed for you or the letter states you received wages from an employer you don't know. If you receive such a letter from the IRS, leading you to believe your identity has been stolen, respond immediately to the name, address or phone number on the IRS notice.
8.	If your tax records are not currently affected by identity theft, but you believe you may be at risk due to a lost wallet, questionable credit card activity, or credit report, you need to provide the IRS with proof of your identity. You should submit a copy of your valid government-issued identification – such as a Social Security card, driver's license, or passport – along with a copy of a police report and/or a completed Form 14039, Identity Theft Affidavit. As an option, you can also contact the IRS Identity Protection Specialized Unit, toll-free at 800-908-4490. You should also follow FTC guidance for reporting identity theft at www.ftc.gov/idtheft
9.	Show your Social Security card to your employer when you start a job or to your financial institution for tax reporting purposes. Do not routinely carry your card or other documents that display your Social Security number.
10.	For more information about identity theft – including information about how to report identity theft, phishing and related fraudulent activity – visit the IRS Identity Theft and Your Tax Records Page, which you can find by searching "Identity Theft" on the IRS.gov home page.

Source: IRS.

The FTC operates a call center for identity theft victims where counselors tell consumers how to protect themselves from identity theft and what to do if their identity has been stolen (1-877-IDTHEFT [1-877-438-4338]; TDD: 1-866-653-4261; or www.ftc.gov/idtheft). The FTC also produces publications on identity theft, including *Take Charge: Fighting Back*

Against Identity Theft.[1] This brochure provides identity theft victims information on

1. immediate steps they can take, such as placing fraud alerts on their credit reports; closing accounts; filing a police report; and filing a complaint with the FTC;
2. their legal rights;
3. how to handle specific problems they may encounter when clearing their name, including disputing fraudulent charges on their credit card accounts; and
4. minimizing recurrences of identity theft.

[1]Federal Trade Commission, *Take Charge: Fighting Back Against Identity Theft* (Washington, D.C., February 2006). This brochure is available at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.htm (accessed May 11, 2011).

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