PREPARED STATEMENT

DOUGLAS H. SHULMAN

COMMISSIONER

INTERNAL REVENUE SERVICE

BEFORE

SUBCOMMITTEE ON GOVERNMENT ORGANIZATION,

EFFICIENCY AND FINANCIAL MANAGEMENT

HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT

REFORM

ON

IDENTITY THEFT

JUNE 2, 2011

Introduction

Chairman Platts, Ranking Member Towns, and Members of the Subcommittee, thank you for the opportunity to appear today to discuss identity theft and how it can affect taxpayers when they interact with the Internal Revenue Service (IRS). I will describe the actions the IRS is taking to detect and prevent taxpayer identity theft, and just as importantly, our efforts to work with and help the victims as best we can.

Since 2009, the IRS has protected $929.3 million in refunds from fraudulent returns from being erroneously sent to identity thieves. At the IRS, we understand the victims' frustrations and are committed to working with them to mitigate the consequences of identity theft. This means identifying identity theft issues affecting the tax filing process and getting the victims the tax refunds to which they are entitled as soon as possible.

We have developed a comprehensive identity theft strategy that is focused on preventing, detecting, and resolving instances of tax-related identity theft crimes. In doing so, we are working to ensure that tax filing issues are resolved, and future instances of such crimes are minimized. To carry out this strategy, we put in place prevention measures to stop identity thieves from taking advantage of unsuspecting taxpayers and established new programs and initiatives to educate and support legitimate taxpayers interacting with the IRS. We have made great progress on both fronts.

I want to emphasize that, by the time we detect and stop a perpetrator from using someone else's personal information for his own benefit, the taxpayer-victim's personal data had already been compromised outside the tax filing process. Thus, the IRS was not the cause of the identity theft. The fraud perpetuated by individuals using a taxpayer's stolen identity should be seen within the context of a much larger problem in the United States and across the globe. The public and private sectors are targets of identity theft, including small businesses, large corporations, banks, and other government agencies.

Identity theft is one of the fastest growing crimes in the United States. In fact, for the 11th year in a row, it was the number one consumer complaint received by the Federal Trade Commission (FTC), the Federal agency that is responsible for protecting consumers against identity theft. The FTC reported that, of the almost 1.4 million complaints received in 2010, 19 percent were related to identity theft. Fraud perpetrated against the government in 2010 was the most common form of reported identity theft crime, followed by credit card fraud. For tax years, 2009 through 2011, the IRS has experienced significant increases in tax issues resulting from taxpayers having their personal identification stolen.

Identity Theft and Tax Administration

There are a number of situations in which tax filings are affected by identity theft. For example, an identity thief uses a legitimate taxpayer's identity to fraudulently file a tax return and claim a refund. Generally, the identity theft perpetrator will use a stolen

Social Security Number (SSN) to file a forged tax return and attempt to obtain a fraudulent refund early in the filing season. The legitimate owner of the SSN may be unaware that this has happened until he files the return later in the filing season and it is discovered that two returns have been filed using the same SSN. We call this type of identity theft a refund-related crime.

Employment-related identity theft is another way in which an identity thief can take advantage of tax information for personal benefit. This occurs when an identity thief uses someone else's name and SSN in the process of obtaining a job. In this situation, the identity thief's employer will report the employee's wage information to the IRS, just as the legitimate taxpayer's employer reports his legitimate wages. However, if the legitimate taxpayer is unaware that an identity thief is using his SSN for employment, the IRS may conclude that he has not properly reported all earned income and a notice of unreported/underreporting income would be generated and sent to the taxpayer. As a result, the legitimate taxpayer must work with the IRS to resolve his account issues and obtain an identity theft marker on his account.

IRS Actions to Combat and Prevent Tax-Related Identity Theft Crimes

As Commissioner, one of my highest priorities is to ensure that taxpayer information is secure and protected. In doing so, we use various techniques to detect and stop refunds on questionable claims. In addition to using internal screening and data mining processes to evaluate returns submitted to the IRS, we also receive referrals from within the IRS and from external sources that are critical to verifying the validity of a return.

In July 2007, the IRS created the Office of Privacy, Information Protection and Data Security (PIPDS) to provide a centralized privacy program. In creating a centralized office, we recognized the need to develop and implement standardized identity theft processes across all IRS organizations.

Our Criminal Investigation (CI) Division also plays a vital role in the IRS' effort to combat identity theft. CI investigates and detects tax fraud and other financial-related fraud, including identity theft, and coordinates with PIPDS and other IRS offices to ensure that false refunds involving identity theft are identified and addressed as quickly as possible, and that the appropriate steps are taken to mark victims' IRS accounts to help prevent future victimization. CI recommends prosecution of refund fraud, including identity theft, to United States Attorney's Office nationwide.

Prevention and Prosecution

The IRS is working to prevent a taxpayer's personal information from being used by someone else before the tax return is processed. Our internal processes check selected information contained in the return against information in our internal databases. If the return is rejected, the legitimate taxpayer has the option of correcting the return and resubmitting it or filing the return by paper. As we move forward, we continue to refine our systems to ensure that the taxpayer's information is protected.

CI investigates cases involving questionable refund schemes, including refund-related identity fraud, and recommends them for prosecution to the Department of Justice (DOJ). For example, in 2010, 41 schemes of national scope were investigated by CI, demonstrating our commitment to pursue prosecutions having a large impact on U.S. taxpayers. Last year, 95 percent of individuals who DOJ prosecuted for refund-related identity theft went to prison.

As a result of our work in combating abuses in this area, there have been a number of convictions involving identity thieves filing false claims for refunds. For example, in 2011, a California woman was sentenced to 30 months in prison, three years of supervised release, and was ordered to pay more than $800,000 in restitution for participating in such a scheme to defraud the IRS. She pleaded guilty to two counts of mail fraud and one count of aggravated identity theft. In 2010, her husband was also

charged in the indictment and was sentenced to 70 months in prison, three years of supervised release, and ordered to pay restitution for his involvement in the scheme.

In 2009, a Florida man and his wife were sentenced to 22 months and 14 months in prison, respectively. Both defendants were ordered to serve three years of supervised release and to pay almost $400,000 in restitution. A year earlier, they were arrested and charged in a 45 count indictment with conspiracy to defraud the United States, filing false claims, misusing SSNs, and aggravated identity theft. The indictment stated that the defendants obtained the personal identifying information of numerous individuals, and used this information to prepare and file fraudulent Federal income tax returns in those individuals' names.

Taxpayer Outreach

The IRS has undertaken several outreach initiatives to provide taxpayers, employees, and other stakeholders with the information they need to prevent and resolve tax-related identity theft issues proactively. We created IRS Form 14039, *IRS Identity Theft Affidavit*, which is used when a taxpayer is an actual or potential victim of identity theft related to a tax filing and would like the IRS to mark his account to identify any questionable activity. The form makes the process easier and less burdensome for taxpayers, particularly because some police departments will not take identity theft reports.

The IRS has partnered with the DOJ and numerous other Federal agencies in the Financial Fraud Enforcement Task Force to address identity theft. The Task Force's website, STOPFRAUD.gov, has information from each agency about what to do if you suspect you are a victim of identity fraud. This partnership also includes pooling investigative resources to investigate identity theft schemes.

The IRS has also featured information on identity theft in our yearly summer tax forums for the practitioner community. Practitioners are typically the first contact, as

more than 8 out of 10 taxpayers use a return preparer or tax software to prepare their returns. At the forums, our management leaders present information to practitioners on identity theft and online fraud detection and prevention. Approximately 14,000 practitioners participate nationwide in these forums.

Lastly, we continually update the IRS.gov website with the latest identity theft information, including emerging trends, phishing sites, fraud schemes, and prevention strategies. The site also provides key information from other Federal agencies, including the FTC. In March 2011, we issued tax tips with the *"Ten Things the IRS Wants You to Know About Identity Theft"* as part of our external communications during the filing season.

Victim Assistance

The IRS recognizes that outreach alone is not enough, and therefore, we also provide significant assistance to taxpayers whose personal information has been stolen and used by a perpetrator in the tax filing process. Beginning in 2008, the IRS implemented new Service-wide identity theft markers that are placed on a taxpayer's account after a taxpayer provides us with certain substantiation documentation. We developed and implemented a total of eight identity theft markers to address unique types of identity theft issues across the IRS. These markers are used to reduce taxpayer burden by (1) distinguishing legitimate returns from fraudulent returns, (2) tracking taxpayers with identity theft-related tax problems and issues encountered by identity theft victims, and (3) preventing victims from facing the same problems every year. To date, we have identified more than 470,000 incidents of identity theft, of varying degrees of severity, affecting more than 390,000 taxpayers.

If the IRS receives multiple tax returns for the same individual(s), the taxpayer will be asked to substantiate his identity to the IRS by providing a copy of a valid Federal or State issued identification, such as a driver's license, or passport, together with a copy of a police report or a completed *IRS Identity Theft Affidavit*. Once we review and verify

the documentation to determine the rightful taxpayer, the return will be processed, and if a refund is due, the taxpayer will receive it. The taxpayer's account will be marked with an identity theft marker to provide additional protection in the future from identity thieves, beginning with the next filing season. We only require this additional documentation where it is not immediately apparent from the face of the tax return which is legitimate. While there is some utility in comparing returns to prior years, the American taxpaying public is extraordinarily mobile and dynamic. Addresses, employers, and family sizes routinely change every year.

Once the initial identity theft case is resolved, IRS computer systems will systematically evaluate future returns submitted on accounts marked with the identity theft marker. If a return has questionable information on it, the return will be manually reviewed to ensure the return was submitted by the legitimate taxpayer and prevent processing of the return if it is believed to have been submitted by an identity thief.

In addition to programming our systems to detect repeat instances of identity theft, we also developed a new program that will help ensure that taxpayers who were subject to identity theft in the past do not encounter delays in processing their tax returns. In January 2011, we began issuing an Identity Protection Personal Identification Number (IP PIN) that these taxpayers will use when filing their future year's return. IP PIN notices were sent to approximately 56,000 taxpayers allowing them to file a return with the IP PIN. We also revised the 1040 series tax forms for the 2010 tax year to allow for the entry of the IP PIN. Taxpayers will receive a letter with a new unique IP PIN each year that the identity theft marker is active on their account.

The purpose of the PIN is to avoid delays in filing and processing Federal tax returns for taxpayers who have been verified by the IRS to be victims of identity theft. This filing season was a pilot year for the program, and it will be expanded to include more taxpayers beginning next filing season.

In 2008, we also established a special unit to serve as a central contact point for taxpayers who had their identities stolen and wanted to notify the IRS. This unit provides a dedicated toll-free number, staffed by English and Spanish-speaking IRS employees, trained to review taxpayers information and account histories, answer questions, and explain the actions necessary to resolve their identity theft issues. Since its inception, the unit successfully provided service to almost 500,000 taxpayers, while maintaining an 83.4 percent level of service.

We also established an online fraud program to address the increasing and evolving threat of online fraud affecting taxpayers. To combat the highly sophisticated attack methods employed by the fraudsters from all around the world, we are proactively looking for web sites and phishing sites posing as the IRS or legitimate e-file providers and shutting them down as soon as possible. Since the beginning of FY 2009, we shut down 8,296 sites, 610 of which have been shut down in FY 2011.

In addition, we established a relationship with the Internet Crime Complaint Center (IC3), a federal working group responsible for investigating Internet crimes, including identity theft. The IC3 receives Internet-related criminal complaints and researches, develops, and refers the criminal complaints to law enforcement and/or regulatory agencies for any investigation they deem to be appropriate. For law enforcement and regulatory agencies, IC3 provides a central referral mechanism for complaints involving Internet-related crimes, like identity theft.

Internal Checks and Balances

Through process modifications, we have implemented operational changes that have streamlined case resolution and reduced taxpayer burden. One example of this is in the circumstance of two returns filed with a single SSN. This situation can occur from honest mistakes, such as keystroke error. However, it could also be the result of identity theft. In the past, when this occurred and the IRS could not make a determination of the true owner of the SSN, we would take a number of steps, including contacting the SSA,

to resolve the issue. These extra steps could often take a significant amount of time. In the interim, refunds associated with the impacted returns could be frozen while a determination of ownership was made. When there was an identity theft, we found that the frozen return would often end up being that of the legitimate owner of the SSN. This was frustrating for both the taxpayer and the IRS as it would make a bad situation worse for the victim. Upon conducting an internal review, we modified our procedures and empowered our employees to exercise judgment based on certain analytical criteria to streamline and improve the process. I believe that these modifications will allow us to improve our turnaround time for taxpayers impacted by identity theft.

In addition, we have developed and implemented a suite of key performance measures to assist in determining the effectiveness and efficiency of our identity theft program. These performance measures are critical to guide the future direction of the identity theft program, and to continuously improve it.

Conclusion

Thank you again, Mr. Chairman, for the opportunity to appear this morning and update the Subcommittee on how tax filing is affected by identity theft. This is an issue that affects millions of Americans each year. It is not only a matter the IRS is confronting, but this is a concern for many other segments of the economy as well.

It is our goal to provide taxpayers with the best possible service to ensure their interactions with the IRS are efficient and that we meet their needs. In all tax-related identity theft crimes, IRS employees work with each taxpayer victim to resolve his unique situation. Identity theft cases are becoming increasingly complex, involving a dedicated review process to ensure we resolve the case satisfactorily for the victim.

As indicated earlier in my testimony, we have taken steps to establish a more consistent, more proficient, and less burdensome manner for handling these cases. We continue to make great progress in preventing tax-related identity theft before it happens,

and stop it when it does happen as quickly and efficiently as possible. We are also constantly looking for new and innovative ways to improve our processes and techniques and recognize that we must work diligently every day to protect taxpayers and ensure that their personal information is safe and secure.