S. HRG. 110–1031

IDENTITY THEFT: WHO'S GOT YOUR NUMBER?

HEARING

BEFORE THE

COMMITTEE ON FINANCE
UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

APRIL 10, 2008

Printed for the use of the Committee on Finance

U.S. GOVERNMENT PRINTING OFFICE

55–978—PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON FINANCE

MAX BAUCUS, Montana, *Chairman*

JOHN D. ROCKEFELLER IV, West Virginia	CHUCK GRASSLEY, Iowa
KENT CONRAD, North Dakota	ORRIN G. HATCH, Utah
JEFF BINGAMAN, New Mexico	OLYMPIA J. SNOWE, Maine
JOHN F. KERRY, Massachusetts	JON KYL, Arizona
BLANCHE L. LINCOLN, Arkansas	GORDON SMITH, Oregon
RON WYDEN, Oregon	JIM BUNNING, Kentucky
CHARLES E. SCHUMER, New York	MIKE CRAPO, Idaho
DEBBIE STABENOW, Michigan	PAT ROBERTS, Kansas
MARIA CANTWELL, Washington	JOHN ENSIGN, Nevada
KEN SALAZAR, Colorado	JOHN E. SUNUNU, New Hampshire

RUSSELL SULLIVAN, *Staff Director*
KOLAN DAVIS, *Republican Staff Director and Chief Counsel*

CONTENTS

OPENING STATEMENTS

WITNESSES

ALPHABETICAL LISTING AND APPENDIX MATERIAL

COMMUNICATION

IDENTITY THEFT: WHO'S GOT YOUR NUMBER?

THURSDAY, APRIL 10, 2008

U.S. SENATE,
COMMITTEE ON FINANCE,
Washington, DC.

The hearing was convened, pursuant to notice, at 10:05 a.m., in room SD–215, Dirksen Senate Office Building, Hon. Max Baucus (chairman of the committee) presiding.

Present: Senator Salazar.

Also present: Democratic staff: Bill Dauster, Deputy Staff Director and General Counsel; Sam Mitchell, Legislative Assistant for Senator Salazar; Mary Baker, Detailee; and Bridget Mallon, Detailee. Republican staff: Steve Robinson, Chief Social Security Advisor; and Nick Wyatt, Tax Staff Assistant.

OPENING STATEMENT OF HON. MAX BAUCUS, A U.S. SENATOR FROM MONTANA, CHAIRMAN, COMMITTEE ON FINANCE

The CHAIRMAN. The hearing will come to order.

A Chinese proverb says, "Make your plans for the year in the spring and your plans for the day early in the morning." Each spring, millions of Americans start to make their plans. Right after they sign their tax returns with a sigh of relief, they begin to plan how to spend their tax refunds. They dream about paying down bills. They dream about buying a new TV. They dream about putting money in the bank. But for tens of thousands of taxpayers each year, their dreams turn into nightmares. These taxpayers are the victims of identity theft.

According to the Federal Trade Commission, during 2006 some 50,000 people complained about tax fraud and employment-related identity theft. That is an increase, a significant increase; 4 years earlier in 2002, there were just 18,000 cases, compared to 50,000 in 2006.

Some taxpayers learn they are victims right away. That is because the IRS rejects their returns; someone has already filed using the taxpayer's name and Social Security number. On average, it takes almost a year for the IRS to sort out who the real taxpayer is. In the meantime, the victim's tax accounts get frozen. The IRS issues no refund. The money that the taxpayer is planning on does not come, and the taxpayer waits in tax limbo for months and months.

Other taxpayers do not learn that they are the victims of identity theft until years later. It is not until the IRS starts matching W–2s to tax returns that the IRS detects the theft. Victims first realize that other people are using their identity when the IRS con-

tacts them and the IRS asks them why they did not report the income that appears on the W–2 forms with their names on it.

Both the National Taxpayer Advocate and the Treasury Inspector General for Tax Administration, otherwise known as TIGTA, have called tax-related identity theft a serious problem. They argue that the IRS lacks adequate agency-wide strategies, strategies to ensure that victims of identity theft are treated consistently and can minimize their burden.

The Advocate has identified at least 17 different functions within the IRS that deal directly with private taxpayer information. The TIGTA has reported as many as 240 computer systems at the IRS that contain personal identifiable information.

Clearly, the IRS requires a comprehensive identity theft strategy with goals, time lines, and milestones. That strategy needs to hold IRS personnel accountable for reducing identity theft. I will call on Commissioner Shulman to provide me with a status report on this in 90 days.

I am amazed that the IRS has no mechanism for taxpayers to give the IRS a heads-up that their identities have been stolen. Instead, the IRS tells victims to report the crime to the Federal Trade Commission, and then the IRS does nothing to coordinate with the FTC to use that information.

I am disappointed that the IRS does not notify a taxpayer when someone else has filed a return using the victim's Social Security number. I am astonished that some IRS processes actually appear to facilitate identity theft. These involve returns filed by persons using individual taxpayer identification numbers, otherwise known as ITINs. These persons will sometimes attach W–2s to returns with someone else's Social Security number.

But ITIN holders usually cannot legally obtain a Social Security number, so returns with both an ITIN and a W–2 with the Social Security number should raise a red flag. But the IRS processes these returns without asking any questions. The IRS deliberately looks the other way. In fact, the IRS changed its electronic filing filters last year so that returns filed using both an ITIN and a Social Security number would not be rejected.

You would think that the IRS would flag those returns, but they do not. You would think that the IRS would notify the rightful owner of the Social Security number that someone else is using that number, but they do not. I am dismayed that the IRS does not do more to stop identity theft. The IRS generally will not prosecute an identity theft case unless it is part of a larger crime.

Victims of identity theft deserve better. They deserve consistent procedures no matter what part of the IRS they are dealing with. They deserve a way to forestall problems with the IRS once they discover they are victims. They deserve to be notified when someone else uses their Social Security number.

Identity theft is serious. It is a crime. It is growing. America's taxpayers must be able to trust that the IRS is doing all that it can to protect their identity. It is time for the IRS to stop stalling. It is time for the IRS to make and implement an effective plan to deter, to detect, and to stop identity theft. It is time to end the nightmare for countless American taxpayers who fall victim to identity theft.

Now we will hear from our witnesses. First, we will hear from IRS Commissioner Doug Shulman, in his debut appearance before this committee as Commissioner. I note that the former Acting Commissioner of the IRS, Linda Stiff, currently the Deputy Commissioner for Services and Enforcement, will join Mr. Shulman at the witness table, although it is my understanding she will not make a statement.

Next, we will hear from Becky Spencer, an enrolled agent from Billings, MT who will tell about the challenges faced by one of her clients, a victim of identity theft. I want to thank you, Becky, very much for taking the time—it is a long distance and expensive—to be here today.

Next is Nina Olson, the IRS National Taxpayer Advocate.

Then we will hear from Russell George, the Treasury Inspector General for Tax Administration, to review TIGTA's findings.

Our usual practice, as I am sure most of you know, is to speak for about 5 minutes, and your statements will be automatically included in the record. I want to apologize in advance that I will have to leave the hearing to attend a conference on the farm bill that was just called yesterday at 7 o'clock in the evening. It is not very good planning, but there it is. But we are very honored and lucky to have Senator Salazar from Colorado to chair the hearing today. Thank you all very much.

Why don't you begin, Mr. Shulman? Thank you.

STATEMENT OF HON. DOUGLAS H. SHULMAN, COMMISSIONER, INTERNAL REVENUE SERVICE, WASHINGTON, DC; ACCOMPANIED BY LINDA STIFF, DEPUTY COMMISSIONER FOR SERVICES AND ENFORCEMENT, INTERNAL REVENUE SERVICE, WASHINGTON, DC

Commissioner SHULMAN. Thank you, Mr. Chairman. I appreciate the opportunity to appear before the committee. This is my first hearing, as you said, before the Senate Finance Committee. I have been on the job under 3 weeks now, and I want to thank you and all the members of the committee for your support during the confirmation process.

As you mentioned, I have asked Linda Stiff to accompany me this morning to make sure we can answer any questions you have, given that I am so new on the job. Let me just say, Linda did an excellent job leading the Agency as Acting Commissioner before I arrived.

My understanding is that this is the annual hearing of the Senate Finance Committee and that you wanted an update on the budget, the filing season, and the stimulus package and payment. Those are included in my written testimony. Therefore, with my limited time, I will make a couple of comments about those issues and then move on quickly to the primary purpose of the hearing: identity theft.

First, I urge members of the committee to support IRS's 2009 budget. That budget has a number of legislative proposals designed to help improve voluntary compliance. I would also like to commend the committee for, last week, releasing a bipartisan discussion draft of the administration's proposal to require information reporting for banks and other entities on reimbursements to mer-

chants that accept electronic forms of payment, including credit cards.

Second, I want to make sure you know we are working hard on getting stimulus payments out to the American people. We expect the first payments to be direct-deposited into taxpayer accounts in early May, with checks going out soon thereafter.

We have also made a concerted effort to reach out to people who normally would not have to file tax returns who may be eligible for stimulus payments to make sure they have all the information they need and help from the IRS to file their return and get their stimulus payment.

Let me now turn to identity theft. My overall goal for the IRS in any area of service is to ensure that, when a taxpayer contacts the IRS with an issue or concern, we have in place a seamless process that gets the issue resolved promptly. From the perspective of an identity theft victim, that means that, when a taxpayer calls the IRS, that they reach someone who is knowledgeable on the issue and is able to take care of the problem quickly and permanently.

I discussed the issue of identity theft with the senior leaders at the IRS my first day on the job 2½ weeks ago. I have also had the opportunity to discuss this issue with Russell George, the head of TIGTA, Nina Olson, the National Taxpayer Advocate, and I believe they both made a number of constructive suggestions to the IRS regarding the handling of identity theft issues.

When I met with the senior staff my first day on the job, they told me, and they agreed with Chairman Baucus, that the IRS is not where it needs to be in meeting the goal of seamless service to taxpayers who are victims of identity theft. They recognized this, and the senior staff of IRS has been working on solutions.

I would like to highlight some of the things that we have worked on most recently to reduce the burden on taxpayers in the event of an identity theft. By this fall, the IRS will have people specially trained to help taxpayers who have been victims of identity theft. When you call the IRS, you will be routed to a specially trained person.

We have also created an office to bring focus and an agency-wide approach to identity theft and data security issues, and have updated agency-wide procedures to make sure that an identity theft victim has consistent treatment when they come into the IRS and identify them as someone who has had their identity stolen.

We also are implementing a new service-wide identity theft indicator that tags the taxpayer's account once identity theft has been established. Once this new process is fully deployed, taxpayers should only have to provide identity theft documentation once, and this will allow a taxpayer to call the IRS and self-identify themselves as a victim of identity theft. IRS will be able to tag it, flag that account, and watch out for further issues of identity theft.

We are also working on making our standards for the documentation we need from a taxpayer to prove that they are that taxpayer easier, so identity theft victims have an easier time with the IRS.

Finally, as Chairman Baucus noted, in the past we did not always identify and tell someone that someone else had used their Social Security number, and we are working on doing that now in

our outgoing communications to taxpayers so they will know if someone else is using their Social Security number.

Finally, we have developed a specialized group of people trained to expedite any identity theft issues related to economic stimulus payments. We want to make sure that everyone who is entitled to an economic stimulus payment receives the payment as soon as possible.

In closing, I want to assure you that Linda and I, as well as our entire leadership team, are committed to continuing to work to reduce the impact of identity theft on taxpayers. We understand the personal devastation that an individual feels when their identity has been stolen. We also understand that, when a victim of identity theft seeks assistance from a government agency, they have a right to expect that that agency will help them, not add to their problem. You have my assurances that we will continue to work diligently to reduce the burden that is placed on taxpayers and the tax system because of identity theft.

Thank you very much. I am happy to answer any questions.

Senator SALAZAR. Thank you, Commissioner Shulman. We appreciate having you in front of the Finance Committee for the first time in your capacity as a confirmed Commissioner of the IRS, and look forward to working with you. We will have a series of questions after we go through the rest of the panel.

[The prepared statement of Commissioner Shulman appears in the appendix.]

Senator SALAZAR. Ms. Spencer?

STATEMENT OF REBECCA SPENCER, ENROLLED AGENT, BENEDICT'S LASER TAX SERVICE, BILLINGS, MT

Ms. SPENCER. Thank you, Chairman Baucus and Ranking Member Grassley, for this opportunity to share my experience regarding tax-related identity theft with the members of the Senate Finance Committee.

In 1975, I took over my uncle's tax practice, and since that time the business has grown to over 6,500 tax clients annually. I am an enrolled agent, and my office was the very first e-filer in the State of Montana.

At first, e-filing was very restricted. Not only did you need a special modem, but there were identity checks and compliance visits to all electronic return originators. But since that time, e-filing has been opened up to the entire world. Anyone with a little prior planning can take a laptop into a cyber café with a stolen Social Security card and a valid Employer Identification Number and file a U.S. income tax return.

On January 14 of this past year, 3 days after e-file opened, one of my long-time tax clients came to the office and filed her tax return. The following morning, we got an IRS acknowledgement that her return had already been filed. Someone had used this single, financially struggling mother of two's identity and filed a tax return on January 13th, well before most people can legally file.

Well, my client, of course, was in tears, and not knowing who to call, I started with the IRS Criminal Investigation 800 number. The recording there states, "If you would like to file Form 3949–A, please order this form by calling 1–800–IRS–FORM. This form

can also be ordered on our website at *www.irs.gov,*" et cetera, et cetera. There is not even an option to leave your name and phone number or to wait for a representative, and previously that wait had been a very long wait.

I called the IRS e-help desk next at the service center, and their response was, "She'll have to file a paper return." Well, next I sent my client down to the local IRS walk-in center, where she was again told to file a paper return. The taxpayer's name and Social Security number were on that return that had been filed, so I thought she should be entitled to a transcript, but she was, in essence, denied access to her own tax account.

The walk-in office could not even help her until she gave them her birth certificate, the FTC form that Senator Baucus talked about, and a written copy of the police report, which took several days for her to get. After that, she was finally referred to the Taxpayer Advocate Service, who finally helped to resolve the case.

Well, the taxpayer was worried that her children's identities had been stolen and that was of great concern, but we were able to find out that that did not happen by calling the Refund Loan Bank. But the bottom line is, 10 days after the Internal Revenue Service had been notified that there was a problem, the Service released that refund to the fraudulent taxpayer, and it was only because the bank I called held the refund until the IRS sorted out who it belonged to that it did not actually get sent to this fraudulent person. Two months later, after contact with at least four IRS functions, the victim finally received her refund.

Now, my office gets calls early in the tax season every year asking to prepare the return from a final pay stub. When we tell them they cannot legally do so, they say, oh, I will just do it myself on the Internet. A taxpayer who is not following the rules only needs last year's Employer Identification Number.

Now, among these early filers are not only the thieves who are outright stealing an identity, but also those who are claiming exemptions that they know the ex-wife is entitled to, or whatever. These returns are a big financial drain on the system because they result in audits, amended returns which must be hand-processed, or, as would have been the case in my example, outright loss of the refund amount.

My client had her identity stolen as a result of a lost government credit card. Does anyone in this room have a government credit card? Based on my experience as an enrolled agent, I have several recommendations for safeguards that the IRS might use to detect and stop identity theft that I would be happy to discuss.

Thank you so very much.

Senator SALAZAR. Thank you very much, Ms. Spencer. Thank you for sharing the real-life stories of people who are affected by identity theft in Montana. Thank you for making the trip from Billings all the way to Washington, DC.

[The prepared statement of Ms. Spencer appears in the appendix.]

Senator SALAZAR. Ms. Olson?

STATEMENT OF NINA OLSON, NATIONAL TAXPAYER ADVOCATE, INTERNAL REVENUE SERVICE, WASHINGTON, DC

Ms. OLSON. Chairman Baucus, Senator Salazar, and members of the committee, thank you for inviting me to testify about identity theft, which is the number-one consumer complaint in the United States today.

In tax administration, identity theft arises when an individual intentionally uses the Social Security number of another person either to fraudulently obtain employment or to file a false tax return in order to obtain a fraudulent refund. In recent years, phishing cases are increasing. That is when someone poses as the IRS, or even the Taxpayer Advocate Service, in order to obtain a recipient's personal information.

I would like to emphasize six key points about identity theft that reflect the taxpayer perspective.

First, identity theft results in serious consequences for the innocent taxpayer. These consequences may include delay or denial of refunds, assessment of tax debts resulting from income reflected on the fraudulent filer's return, and a requirement for victims to prove their identity to the IRS year after year.

Second, the IRS has no idea how many cases of tax-related identity theft exist. Until this year, the IRS had no method to systemically track identity theft cases. Its new procedures, while they represent a good first step, will still result in a substantial undercounting of identity theft cases. Based on the cases we have seen in the Taxpayer Advocate Service, the problem is far more widespread than the available IRS data suggests.

Third, the procedures for handling identity theft cases are unduly burdensome to taxpayers and need to be improved. Let me describe some key points. When a taxpayer first contacts the IRS due to a delayed refund or in response to an examination or a collection notice for income that the taxpayer did not earn, the taxpayer generally does not know that he or she is the victim of identity theft.

The IRS customer service representative will observe a duplicate return filing on the IRS data system and generate a letter to all persons who use the SSN, informing each that there may be a problem with the SSN used on the return, requesting proof of identity and including a questionnaire about the filer's past use of the SSN.

If none or all of the SSN users respond to the first letter within 40 days, the IRS assigns a temporary IRS number, or IRSN, to each user of the SSN, including the identity theft victim. The IRS then sends a second letter that must appear extremely confusing to taxpayers. In that letter, the IRS first tells the taxpayer that he must use an IRSN, and second, tells the taxpayer that because he is using an IRSN he will not receive the Earned Income Tax Credit or the Child Credit, or other such benefits until the IRS can straighten out the SSN, and finally tells the taxpayer that he should claim those credits anyway using the IRSN on the return. These instructions undoubtedly confuse many taxpayers and may intimidate others, making them less likely to claim the EITC or other tax benefits.

The IRS does not call taxpayers to discuss any of these developments. All communication is done by correspondence, which might

be incomprehensible to someone with low literacy. The phone number listed on the letter is usually a toll call for the taxpayer, which might deter a low-income taxpayer from calling for assistance. Basically, IRS needs to think about the taxpayer when designing its procedures.

Fourth, the IRS's new identity theft indicator, which I have long advocated, will reduce the burden on taxpayers who experience identity theft in recurring years by placing an indicator on their account once they have proved their identity the first time. However, the IRS has no central guidance about how to apply the indicator, thus an identity theft victim's account may be handled differently depending on which part of the IRS he or she contacts.

Fifth, the IRS does not follow coordinated procedures that can address an identity theft victim's issues from start to finish. Multiple IRS functions work on various aspects of identity theft cases, but no function is responsible for addressing all Federal tax issues to make the taxpayer whole.

In my 2007 report to Congress I recommended that the IRS develop a dedicated centralized unit to handle all identity theft cases and a centralized chapter in the Internal Revenue Manual to house all identity theft procedures. A centralized unit will be able to identify trends and systemic problems and can serve as a central point of contact for discussions with the Social Security Administration to improve processing.

Victims of identity theft would have a single point of entry into the IRS and could more readily check on the status of their identity theft-related account issues. All IRS functions could coordinate with that function to better assist identity theft victims, regardless of their specific tax problem.

Finally, I commend the Treasury Department for issuing regulations that will reduce the risk of identity theft overseas. In recent years accounting firms have increasingly been outsourcing return preparation to preparers located in other countries. While section 7216 of the code generally makes it a criminal offense for a tax preparer to disclose tax information to third parties, the U.S. Government cannot reasonably enforce that law overseas. This puts a taxpayer's personal information at greater risk of being sold or misused. The recently issued regulations adopt a very balanced approach by allowing U.S. preparers to share most of the taxpayer's tax return information overseas with the taxpayer's consent, but requiring preparers to redact the taxpayer's SSN.

Thank you. I will be glad to answer any questions.

Senator SALAZAR. Thank you, Ms. Olson.

[The prepared statement of Ms. Olson appears in the appendix.]

Senator SALAZAR. The Honorable Russell George.

STATEMENT OF HON. J. RUSSELL GEORGE, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, DEPARTMENT OF TREASURY, WASHINGTON, DC

Mr. GEORGE. Thank you, Senator Salazar. I would also like to thank Chairman Baucus for the opportunity to testify on the growing problem identity theft poses to the administration of our Nation's tax system.

Each year more than 130 million taxpayers entrust the IRS with their sensitive financial and personal data that are stored in, and processed by, IRS computer systems. The risk that this sensitive data could be compromised continues to increase. Most of the IRS's approximately 100,000 employees and contractors have access to at least some of this information on a daily basis. Both internal factors, such as the increased connectivity of computer systems and greater use of portable laptop computers, and external factors, such as a volatile threat environment related to increased phishing scams and hacker activity, contribute to these risks.

Insider attacks by employees and contractors continue to be a concern because employees and contractors are more familiar with the IRS network than outsiders and can potentially do more harm. TIGTA's penetration tests on the IRS's internal network have shown that disgruntled employees and contractors could gain unauthorized access to passwords and sensitive systems data due to high-risk vulnerabilities, which are also well-known to the hacker community.

There are two primary types of identity theft related to tax administration. The first involves an individual who steals another person's name and Social Security number to file a fraudulent tax return in order to steal a tax refund. The second type, employment identity theft, involves an individual who uses someone else's identity to obtain employment which results in taxable income reported to the wrong taxpayer.

As noted by Chairman Baucus, the Federal Trade Commission reported that in 2007 more than 56,000 people complained that they had been victimized by one of these two types of identity theft. The IRS's identity theft program has primarily focused on public outreach and education. However, its processes and procedures have been inadequate in reducing the burden for taxpayers who have been victimized.

When the IRS becomes aware of employment-related identity theft, it does not take action unless the case directly relates to a substantive tax or conspiracy violation. The IRS cannot notify employers when it has information which indicates that an employee may be using another person's identity to obtain employment because of restrictive confidentiality and disclosure provisions in the tax code.

Other systemic problems also hamper the IRS's ability to ensure the security of sensitive taxpayer information. For example, the IRS does not collect all transactions and audit trails on its modernized systems. This type of review is needed to determine whether IRS employees are illegally browsing through taxpayer files.

The IRS is deploying new systems that lack detection capabilities. Without these audit logs, the IRS does not know what configuration changes were made, or who makes them. Intruders and ill-intended IRS employees who have access to these components could steal taxpayer information with little chance of detection.

To compound the risk that personal information could be lost or stolen, some IRS employees regularly take laptop computers containing sensitive information outside their offices to carry out their audit or collection duties. To address these challenges, security must become part of the fabric of the IRS.

In September of last year, TIGTA reported that managers continue to give employees access to systems they do not need to carry out their job responsibilities. Because the IRS sends sensitive taxpayer and administrative information across its networks, routers on the networks must have sufficient security controls to detect and deter unauthorized use.

TIGTA found that access controls for IRS routers were not adequate, and reviews to monitor security configuration changes were not conducted to identify inappropriate use. Essentially, the IRS had no idea who had access to its network components.

We have recently reported that the IRS has not placed sufficient emphasis on employment-related and tax fraud identity theft strategies. Its prevention strategy does not include pursuing individuals using another person's identity unless a given case directly relates to a substantive tax or conspiracy violation, as I noted.

According to IRS policy, the actual crime of identity theft will only be investigated by its Criminal Investigation Division if the crime is committed in conjunction with other criminal offenses having a large tax effect.

In fiscal years 2005 and 2006, the IRS recommended only 45 and 55 cases, respectively, for prosecution that included charges of identity theft. In addition, actions taken in response to employment-related identity theft are not adequate to stop the unlawful use of the identity. Although the Social Security Administration notifies employers of mismatches between names and Social Security numbers, the IRS does not. A serious problem develops for lawful taxpayers when both their names and Social Security numbers are used by others to gain employment.

Because the IRS and the Social Security Administration assume that the information on an employee's W–2 form is accurate, the earnings resulting from the identity theft will be attributed to the lawful taxpayer for determining both Social Security and tax liabilities. The IRS does not pursue the taxes that might be due on income earned using a stolen identity because it contends it does not have sufficient enforcement resources to address most of the identity theft cases.

Furthermore, the IRS holds that it is not worthwhile to pursue enforcement of employment-related identity theft cases for unreported tax liabilities because the taxes owed in most of these cases are not significant. TIGTA is concerned that if the IRS takes no additional action to address the misreporting of income resulting from identity theft, there is no deterrent to keep the problem from spreading.

The IRS advised TIGTA that it is implementing a 5-year strategy for its Privacy, Information Protection, and Data Security Office that will include identity theft issues. However, it did not state when this strategy will be implemented, what milestones will be established, and how its success will be measured.

Overall, the IRS lacks the comprehensive data needed to determine the impact of identity theft on tax administration. It also faces enormous challenges of securing the vast amount of personally identifiable taxpayer information that it stores.

I hope my discussion of tax-related identity theft will assist you with your oversight of the IRS. Thank you, Senator Salazar.

Senator SALAZAR. Thank you, Mr. George. We appreciate your testimony.

[The prepared statement of Mr. George appears in the appendix.]

Senator SALAZAR. Chairman Baucus, first of all, chaired this hearing at the outset, but as he indicated, we have worked long and hard on a very important piece of legislation, and that is the farm bill, which has been 3 years in the making, and he is a spearhead of that conference and we need to make sure we are represented there, so that is why he is there and I am here, because it takes about 26 years to make it from the end of the table to here. [Laughter.]

And Ranking Member Grassley is, I think, also participating in that conference, and also has a Judiciary Committee hearing, as I understand it.

So I am going to make my own statement, and then I have a series of questions from both the chairman, as well as myself.

OPENING STATEMENT OF HON. KEN SALAZAR, A U.S. SENATOR FROM COLORADO

Senator SALAZAR. Today's hearing marks the Finance Committee's annual examination of issues and challenges related to tax filing season. It is the time of year when many Americans are working very hard to complete their tax returns in order to submit them to the IRS prior to that dreaded deadline of April 15th.

Given the complexity of the process, the importance of getting it right, and the sensitivity of the information contained in those returns, tax filing season has a number of important implications that deserve to be examined in greater detail. Therefore, I appreciate Chairman Baucus and Ranking Member Grassley's decision to hold this hearing at this time during tax season.

One of the issues we examined at last year's tax filing season hearing was the ease with which criminals can access taxpayers' private personal information and use it to file a fraudulent tax return with the goal of receiving a tax refund that is not rightfully theirs. These scenarios present particularly difficult challenges to the IRS, which must work to crack down on fraud of this kind while continuing to be as responsive and user-friendly as possible to law-abiding citizens.

This focus that we have this year on identity thieves, but more importantly on their victims, is something that is important for all of us. I hope we can continue to examine how we can improve the system and that the report that Chairman Baucus requested of you, Commissioner Shulman, within 90 days, will hopefully address some of the issues and concerns and recommendations that we have heard from the rest of the panel here.

I served as Attorney General of my State of Colorado for about 6 years and worked with the National Association of Attorneys General and others with respect to the growing issue of identity theft. It certainly goes beyond what happened with the IRS with respect to tax refunds, but also we have seen, especially in the new age of the Internet, and technology, and e-filing, that what we are looking at is really the number-one consumer protection complaint that we have across the country, and it seems to me, based on the

testimony that we have heard here this morning, that that is being seen here with respect to the IRS.

Let me start out with you, Mr. Shulman. First of all, you heard from Ms. Spencer, Ms. Olson, and I think Mr. George with respect to what they consider to be an inadequate response on the part of the IRS whenever you have a victim. You can imagine anyone out there, including the mother that Ms. Spencer described, being a victim of identity theft, calling the 800 number and essentially going into the "La-La Land" of talking to robots and not being able to talk to a person. And the frustration that that mother must have felt is probably felt by every single person who is a victim of identity theft with respect to their tax refund.

So give us, if you will, the highlights of how it is that you intend to address the concerns of being an advocate for the victim as Commissioner of the IRS.

Commissioner SHULMAN. Yes. Thank you, Senator, for the question. Let me first, on behalf of the IRS, say to Ms. Spencer that she should pass along that your taxpayer should be treated better. We recognize that and we are working on it. So, our apologies for the experience that she went through. Also, it is always helpful, as we talked about in my confirmation hearing—we are a big government agency, we have 106,000 people, we have important jobs to do—to make sure we understand the personal stories of people so that we are helping people and citizens get through to and work with us.

I think that I outlined a number of steps that we are taking, a lot of them being ones that I think Mr. George and Ms. Olson, in their testimony, pointed out we should be doing. As I told you, Linda has been an incredibly strong leader, whom I think shares my belief that we should always be getting better and we should view people like Ms. Olson and Mr. George as strategic assets of the IRS, who can point out where we can get better. They have ideas, and we have the resources and the means to improve them.

I think one is, we are going to have specialized people in place at the IRS by this fall who would have been able to answer and sort through all the issues at the IRS that Ms. Spencer's client experienced. So it will not be just going out to the masses and having different divisions working, and you will have a person that you will get to who is specially trained by this fall.

Second, there is this issue that——

Senator SALAZAR. Let me ask you, just on that, Commissioner Shulman. Will someone like Ms. Spencer's client, once you have that system up, have the ability to contact a person directly and actually get to talk to a person immediately upon making that phone call?

Commissioner SHULMAN. Yes.

Senator SALAZAR. Or are we still going to be dealing with voice mail and other recordings where you are not going to have that kind of human interaction? It seems to me that in these kinds of circumstances what people want to do is, they want to have a dialogue with somebody who is going to be able to guide them as opposed to entering into this land of no response.

Commissioner SHULMAN. This will be getting to a person who can help sort through your issue.

Senator SALAZAR. In other circumstances, domestic violence circumstances, other criminal jurisdiction issues, one of the things that we have done on the consumer protection side, at least, when I was Attorney General was to set up hot-lines to address these kinds of issues. Will we have that kind of a capability here where, if you have somebody who has been a victim of identity theft, that they will be able to easily access a certain number and talk to a real-life person?

Commissioner SHULMAN. There will be a clear place on the website for those who prefer to use the Web, and two, there is the 800 number. If you say the words "identity theft," you will be sent to a person who is trained to deal with identity theft victims.

Senator SALAZAR. And will we have enough personnel within that station to be able to make sure that you do have a human voice and a human response to that victim?

Commissioner SHULMAN. That is my goal. As you know, I am 3 weeks onto the job. My answer will be yes, but I need to look at resources and make sure how we allocate them so we have people there.

Senator SALAZAR. This goes to another related question, and that is one of the things that Ms. Olson testified to—her conclusion that we do not have any sense of the quantum of the problem. The IRS does not have any sense of how many people out there are victims of identity theft. Do you have a sense of that, or does Ms. Stiff have a sense of how big the problem is?

Commissioner SHULMAN. What Ms. Olson pointed out, correctly, is identity theft is a rapidly emerging issue. The IRS has looked at identity theft in relation to tax issues, so it had not been tracking this as identity theft, it had been saying, this is somebody who is using somebody else's Social Security number. I think we now have heightened awareness about this and are starting to collect information. In the past, we had not coded and tagged cases as "this is identity theft." We coded them as "this is a double use of a Social Security number," which, in general, is identity theft. So we are now starting and going forward to identify that.

Senator SALAZAR. Going forward. Commissioner Shulman, the reality is, we do not know how many victims of identity theft there are with respect to the IRS today. So as you look, Commissioner Shulman, at putting together the kind of fast-response team to provide relief to victims of identity theft, how are you going to size that team to make sure that you are allocating the resources that that team would need to be able to provide the hot-line, quick, effective human response to a victim of identity theft?

Commissioner SHULMAN. Well, right now what we will do is make sure that we have a number of people trained enough to respond to our current sense of identity theft, and then you just do some over-staffing so people will also be available—the over-staff—to deal with other taxpayer issues if they come in. But they will be 100-percent trained to deal with identity theft. So, I think there are ways.

And one thing I have learned, because I have paid a lot of attention to how we are manning the phones for economic stimulus payments, is we have a very sophisticated ability to deploy people in real time to answer phones around questions, and to adjust those

on a daily basis based on volume coming in. So we will train enough people to deal with it. We will over-staff, but those people will also be available for other issues in case identity theft claims are not coming in.

Senator SALAZAR. So, if we call, when can we test your system?

Commissioner SHULMAN. This will be ready this fall.

Senator SALAZAR. So, this fall. September? October? Let us assume we are in Ms. Spencer's client's shoes. If we were to call, we would be able to find that function up and running and effective in September?

Commissioner SHULMAN. I will come back to you with a date. I will tell you, I have been here 3 weeks. I sat down with the team. I agree with you that we need time lines and deadlines. I pushed the team, the same team that is doing all the calls around the stimulus package. They promised me by this fall, and I will be able to give you an exact date within a couple of weeks.

Senator SALAZAR. All right.

Again, to you, Commissioner Shulman. Ms. Spencer testified that 10 days—10 days is a long time of waiting, long nights—after her client reported the theft of her identity to the IRS, the IRS released the refund to the fraudulent filer. Ten days. It was only because Ms. Spencer took the initiative to call the bank that the refund was not sent to the identity thief, not because of anything the IRS had done.

Can you tell me how that was allowed to happen, and why did the IRS not immediately put a freeze on the refund after the taxpayer notified the IRS about the problem?

Commissioner SHULMAN. This is the first I have heard of this case, and so I cannot comment on this specific case and how this happened.

Senator SALAZAR. In general, if you had a case like this, why would you not just immediately put a freeze on that refund to avoid, if you will, the growing difficulty and the ultimate victimization?

Commissioner SHULMAN. I am going to ask Ms. Stiff to help me on this one.

Ms. STIFF. We have a number of procedures in place to enable us to process 200 million tax returns a year. What you are suggesting is something that will be part of what we are looking at as we approach next year's filing season, but our systems, as they stand today, those refunds are going through in bulk. We do not freeze every time there is an indication of a problem because the bulk of these we research and satisfactorily resolve. So we are having to evolve our processes as identity theft grows, because maybe the procedures we have in place are not adequate to be responsive in a timely manner to the growing number of identity theft cases.

Senator SALAZAR. Ms. Olson and Mr. George, do you have a comment on that question?

Ms. OLSON. I think that I was speaking to my employees in Birmingham, in my Birmingham, AL office, and they told me of a similar situation where they had received a call. They noticed that the first refund was scheduled to go out, called the IRS, called Criminal Investigation and asked them to freeze that refund, and they said, we do not work identity theft cases. I think that if you

have this centralized unit that is trained, then you will be able to develop systems that they will be able to look at and see if a refund is scheduled to go out, and then we would have to develop the capacity to individually stop that refund. Or, if it is too far along in the process——

Senator SALAZAR. You are the National Taxpayer Advocate. So what Commissioner Shulman is attempting to do is to develop a plan to address identity theft. You had six recommendations for him. You are going on now with respect to one of those recommendations. Are you involved in helping them develop a comprehensive response to the identity theft issue that we are talking about here today?

Ms. OLSON. I have been invited, and I have given them a name on our staff to work with on this, and I have been informed that my staff has not yet been involved in these proposals.

Senator SALAZAR. Why is that, Mr. Shulman?

Commissioner SHULMAN. As I told you, I have had the opportunity to sit down with Ms. Olson, now, twice in my 2½ weeks here, and I plan to involve her in these discussions. I have no knowledge about staff-referred proposals. But we have been working hard on this, and we are committed. As I said, I view her as a strategic asset in working with taxpayers.

Senator SALAZAR. I would imagine that, at the end of the day, we are all on the same team here in terms of trying to avoid identity theft. So having all of those who have recommendations and will have insight—whether it is Ms. Olson or Mr. George—involved in putting together this plan to address the issue, would seem to make sense.

Commissioner SHULMAN. Yes. You have no argument with me on that, sir.

Senator SALAZAR. All right.

Mr. George?

Mr. GEORGE. I just simply want to say that I do not know whether this would have affected Ms. Spencer's example, but the IRS has a program called Questionable Refund Program that recently changed its policies in terms of whether or not it would freeze the refunds of tax returns that were questionable in the past, that had a hint of impropriety. So, I believe that it is due to recommendations of Ms. Olson that that policy was changed. So I do not know whether that is something that the IRS needs to revisit, but it might again help in a situation such as what was described earlier.

Senator SALAZAR. All right. Thank you.

Ms. Spencer?

Ms. SPENCER. Well, one of the things that has frustrated me for a long time as a return preparer in a large office is that when we have these kind of issues, there is not a special mail stop at the service center for us to send the paperwork to, along with the proof, and have things expedited. There is absolutely nothing in the system to do this. As far as this refund going out, I was told by my State Taxpayer Advocate office, because I did ask, that it has been turned over to Financial Management, and Financial Management cannot stop a refund. So, you have no window at all. It is just, once it gets accepted by the IRS, that is the end of it. The case is home free.

Senator SALAZAR. I appreciate that observation and your real-life conclusion there, Ms. Spencer.

Commissioner Shulman, on dollars that the IRS sends out on erroneous refunds every year in identity theft cases, do we have a quantification of how much that is?

Commissioner SHULMAN. I do not think we do. Could I make just one comment on the last set of issues about refunds getting frozen, going out, and just give you an observation that I have after 2 weeks on the job?

Senator SALAZAR. Sure.

Commissioner SHULMAN. We have this dueling tension that I think Mr. George was referring to, which is, one, to make sure that we protect the fisc in the National Treasury and bring in all the dollars that we need and not send out any fraudulent refunds. Two is to treat taxpayers well. So this issue has come up in other contexts already where there has been criticism of the IRS for holding a refund if it did not have all the facts and circumstances and someone was not given their due process rights. I think that is what you were referring to, Mr. George, a change in policy to push things out faster.

So these are issues that the Service grapples with every day: how do you get refunds out very quickly to people and make sure you are not getting them out to fraudulent people? It is just a tension that our people are well aware of in trying to strike the right balance.

Senator SALAZAR. Let me ask you a series of questions that really relate to the concept of trying to create some kind of an identity theft crisis center within the IRS. If we had an identity theft crisis center in the IRS, would that be helpful to address some of the issues that have been raised by Ms. Spencer and Ms. Olson and Mr. George? I do not understand, frankly, why the IRS cannot have a one-stop office that can handle these kinds of cases. It seems to me that, if you discover a victim of identity theft, people want to know about that as soon as possible.

Yet, when I hear the description of what went on with Ms. Spencer's client and what Ms. Olson had to say, first she went to the IRS website and was told to file a complaint with the Federal Trade Commission. They also were given the toll-free number from the IRS. Yet, according to TIGTA, the IRS does nothing with the FTC data. So this seems to me that we need a new mechanism, a new organization that can be effective at addressing the victimization of identity theft victims.

So I guess I ask that as a question. I would like a comment from you, Commissioner Shulman. But it just seems to me that this is an opportunity for you as the new Commissioner of the IRS to look at this in a comprehensive fashion that addresses many of the issues and concerns that have been raised by our other witnesses today, as well as by Chairman Baucus in his opening statement this morning.

Commissioner SHULMAN. Yes. You have my commitment to look at this in a comprehensive fashion. I also will tell you, I was heartened my first day on the job when Linda said, we do not think we are far enough along, and we are working on it. Now I am going to get the focus of the top people of the IRS, and I will commit to

the request that the chairman made, that in 90 days we will come back with a comprehensive plan.

Senator SALAZAR. Let me ask a question of your coordination from the IRS to Department of the Treasury and other law enforcement agencies. It is obvious to me that the Department of Justice has a major set of issues with respect to identity theft. Is there a coordination that occurs, Commissioner Shulman and Mr. George, with respect to other agencies outside of the Department of Treasury whenever you have identity theft that you have identified occurring?

Mr. GEORGE. To some extent there is, Senator. The Department of Justice has taken the lead in certain areas, but the Social Security Administration has an agreement, a memorandum of understanding, with the Department of the Treasury allowing for the exchange of certain information. It has to be noted, however, that there is a provision within the Internal Revenue Code, section 6103, that places strict limitations on the types of information that can be shared, which include criminal penalties if violated. So, while this is a tax policy issue that the Commissioner would need to discuss with the Assistant Secretary for Tax Policy at the Department of Treasury, there are ways to address the issue that you are raising.

Senator SALAZAR. Ms. Spencer, you have had 30 years of experience working in this arena. At the very end of your testimony, you said that you had some recommendations that you would make to the IRS and to us in terms of how they address the identity theft issue. Can you highlight what those recommendations are?

Ms. SPENCER. Well, first of all, I would like to say that I have actually had more like 40. About 30 years ago, Senator Baucus, or this committee, suggested that Social Security numbers be put on tax returns for all dependents, and that had not previously been done. They found out that first year that there were a lot of duplicate Marys and Johns and Dicks, and all those common names. I cannot remember how many dependents fell off the tax rolls. It was millions. Two million is the figure that stands in my mind. And the IRS did not do anything with that Social Security information for over 10 years, but those duplicate children fell off and stayed off.

When you think of making change, it often is, well, no, they cannot do that because they do not have the systems in place. But if the rules are there, whether the systems are in place or not, I think it helps to deter the thieves.

One of the things that I feel would be helpful would be to require the W–2s to be sent in to Treasury—electronically, at least—before the employees are given the W–2s, instead of 1 month later. Why can these things not be at a certain time, and then not open the e-file up to the general public until those W–2s have to be released? When people go to paid preparers now, if we are doing electronic filing, particularly, the Service is asking us to get picture ID and copies of Social Security cards, and those things are not being asked of these people who are using this Free File Alliance.

If, annually, the W–2s had to have something as simple as a two-letter code that you gave to each employer and then that was matched so that you knew they had a new W–2 instead of last year's W–2, I think that might help to prevent people from using

that prior year's W–2 to jump the gun on their filing, or to steal a last year's W–2.

Another thing. If people do their own filing on the Internet, if they just had to scan W–2s into the software, or perhaps fax them to a dead-end fax number, I believe that the dishonest would not be quite so prone to add another digit to their withholding, or that sort of thing. I mentioned about the electronic return originators having a special mail stop to go to for problem returns. But another thing that dropped off, and I am not sure if it was last year or the year before, prior year adjusted gross income does not have to be put on the return by self-prepared returns.

Senator SALAZAR. Ms. Spencer, I just was informed that a vote has just started, so we have about 3 or 4 minutes here with the hearing. But I want to just invite you to provide those recommendations both for this committee, as well as to Commissioner Shulman, so that they can be considered as he revamps the effort.

Let me ask Ms. Olson just a question related to tax preparation being outsourced to overseas locations. How big of a risk does that create, and can you quickly sort of describe the risk and what it is that the IRS ought to be doing with respect to this outsourcing?

Ms. OLSON. Well, this issue came up in talking about how preparers use or disclose the information that they receive from the client. In the most recent years as accounting firms, both large, medium and small, have been outsourcing return preparation to places overseas, many people have been raising questions: what happens to that information once it is out of the country?

The Taxpayer Advocacy Panel, which is a Federal advisory committee chartered to advise the Commissioner, the Secretary, and myself on taxpayer issues—and they are volunteer taxpayers, lay people, generally, who make these recommendations—really made this a primary concern of theirs, that they were very concerned about this practice.

So the current Treasury regulation basically says that, if you are sharing information overseas for return preparation, if you are outsourcing, it does not ban the outsourcing itself because that is a business practice, but that we want you to mask the SSN so that in some way you do not link the financial information, the address, to that all-important number which would allow you to essentially, overseas, steal someone's identity. The problem is, overseas our laws do not reach.

Senator SALAZAR. Thank you, Ms. Olson.

Mr. George, how well does the IRS protect taxpayer data, and what more should the IRS be doing to ensure that confidential taxpayer information is protected?

Mr. GEORGE. In all honesty, Senator, this answer would require a lot more time than I think we have today. I have seen examples recently, sir, where the IRS is using commercial vendors to transport sensitive tax data that is being misdelivered to people and who are allowed to look at tax returns that they should not have access to. The bottom line is, there is not a sufficient strategy within the IRS in terms of protecting the data. I am hopeful, hearing what Commissioner Shulman has indicated today, that he is dedicated to addressing this issue.

I am committed to working with them, as I am certain that everyone else on this panel is. But not enough is being done. All you need is a single laptop stolen which could contain tens of thousands of taxpayers' sensitive information, and that in and of itself could cause a catastrophe to the lives of people involved.

Senator SALAZAR. We would appreciate your work on the plan that Commissioner Shulman will put together for Chairman Baucus to make sure that your input is considered in that plan.

I would say a comment here in closing before I adjourn the hearing. It seems to me that one of the things, Commissioner Shulman, you might want to consider as you put together this plan is an identity theft crisis center, because I think for those who are victims of identity theft, they do end up being in a significant crisis when they find out their identity has been stolen, or they find out they are not going to be getting their tax refund. You want to be able to provide them the kind of relief that we try to provide in the criminal justice system, frankly, to people who have been the victims, in this case, of a crime.

Second of all, it seems to me that, given the nature of identity theft, that this is an issue where we have many fingers of the government involved in trying to deal with identity theft in all of our agencies, whether it is Homeland Security, whether it is other elements of Department of the Treasury. So there may be lots of assistance that you can get from some of the other Federal agencies that are involved in this issue, and I would think that, for example, the Department of Justice has a very significant interest in going after and prosecuting those who are the criminals who are ultimately committing identity theft.

Let me thank you all as witnesses for coming before the Senate Finance Committee and providing us with your testimony. We look forward to working with all of you.

The hearing is adjourned.

[Whereupon, at 11:08 a.m., the hearing was concluded.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

SENATOR JOHN ENSIGN
Identity Theft: Who's Got Your Number?
April 10, 2008

Mr. Chairman, thank you for holding this hearing on identity theft. As you may recall, I have long been concerned about identity theft, and have offered multiple amendments to multiple bills to reduce document fraud, prevent identity theft, and preserve the integrity of the Social Security system. I have also worked to prohibit the Internal Revenue Service (IRS) from sending Economic Stimulus rebates to individuals who do not have a valid Social Security number.

Mr. Chairman, there have been many media reports about illegal immigrants stealing Americans' Social Security numbers. To understand the potential scope of this problem, you have to understand that every year employers are advised that nearly 800,000 employees do not have valid, matching Social Security numbers. In too many cases, the number used belongs to someone else. We need to consider the impact that crime has on the victim.

Identify theft by illegal aliens has created many problems for Americans. Sometimes those problems involve the Internal Revenue Service. Last year, I spoke on the Senate Floor about Audra, a stay-at-home mom since 2000. The IRS had accused her of owing $1 million in back taxes. Audra had not worked in six years. Yet, the IRS said she owed taxes for working the last three years. What she first thought was a mistake, later became clear. It was a case of identity theft. Her Social Security number was being used by at least 218 illegal immigrants, mostly in Texas, to obtain jobs.

Audra isn't the only victim. In Fiscal Year 2006, the IRS had 16,152 cases of mismatched names and Social Security numbers. These cases occur when an individual uses someone else's Social Security Number (often to gain employment), but not the victim's name. Ultimately, the victim learns about the identity theft when the IRS contacts him about his unreported income, which could be months or even years later.

Mr. Chairman, identify theft by illegal aliens has damaged many Americans' credit, making it hard to buy the basic necessities. In some cases, the victims of identity theft are denied social service benefits – like unemployment – because records show they have a job. In some cases, government records show they have many jobs – all across the country. Last year, I told my colleagues about Caleb who lives in Northern Nevada with his wife and two young children. Caleb is one of my constituents.

In December 2003, Caleb was unable to work and applied for unemployment benefits. He was denied benefits and told it was because he was told he was already working as a landscaper in Las Vegas. Many of my colleagues are probably not familiar with the geography of Nevada. I am pretty confident that Caleb was not living in Reno and commuting to Las Vegas to work every day. If he was, his round trip commute each day would be nearly ONE THOUSAND miles.

Stories like Caleb's are all too common. Many Southwest states, like Utah and Arizona, and even my home state of Nevada, have experienced a crime spree involving illegal immigrants using the stolen identities of children. In one case in Utah, a child apparently owns a cleaning company and works as a prep cook at two restaurants in Salt Lake City. That's a lot of responsibility – especially for an eight-year-old boy. Another boy from Salt Lake City supposedly works for an express air freight company. Quite an important job for an 11-year-old.

Mr. Chairman, the stories about Social Security fraud and identity theft are shocking. It is clear that illegal immigrants are purchasing false papers and using stolen Social Security numbers to obtain jobs. And, they are victimizing hard-working Americans, denying the opportunity to Americans who want to work, and are victimizing young children in the process.

I am extremely interested in learning more about the IRS' process to address identity theft and am eager to engage in a discussion to improve our nation's identity theft strategy. It seems to me that more identity theft coordination is needed within IRS and between IRS, the Social Security Administration, and the Department of Homeland Security. I look forward to working with these agencies to help prevent identity theft and protect the integrity of our tax system.

Thank you, Mr. Chairman.

STATEMENT OF
THE HONORABLE J. RUSSELL GEORGE
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
U.S. SENATE
COMMITTEE ON FINANCE

April 10, 2008

Chairman Baucus, Ranking Member Grassley, and Members of the Committee, thank you for the opportunity to testify on the growing problem of the threat identity theft poses to the administration of our nation's tax system. My comments will focus on the Internal Revenue Service's (IRS) efforts to protect the personally identifiable information of millions of taxpayers, the IRS's efforts to assist taxpayers who have been victimized by identity theft, and its ability to identify fraudulent returns. My closing comments will briefly address the status of the 2008 Filing Season.

In the context of this testimony, as is generally agreed, identity theft occurs when someone steals and uses someone else's personally identifiable information (PII) – his or her name, Social Security Number, credit card numbers, or other forms of financial information.

There are two primary types of identity theft related to tax administration: The first involves an individual who steals another person's name and Social Security Number to file a fraudulent tax return in order to steal a tax refund. The second type – employment identity theft – involves an individual who uses someone else's identity to obtain employment which results in taxable income reported to the wrong taxpayer. The Federal Trade Commission (FTC), the primary Federal agency responsible for receiving identity theft complaints, reported that in 2007, more than 56,000 people complained that they had been victimized by one of these two types of identity theft.[1]

The IRS's identity theft program has primarily focused on public outreach and education. At the same time, however, its processes and procedures have been inadequate in reducing the burden for taxpayers who have been victimized.

When the IRS becomes aware of employment-related identity theft, it does not take action unless the case directly relates to a substantive tax or conspiracy violation. The IRS cannot notify employers when it has information which indicates that an employee may be using another person's identity to obtain employment. Internal Revenue Code confidentiality and disclosure provisions restrict the IRS's ability to share employee information with his or her employer. However, there are exceptions in the Internal Revenue Code that allow disclosure of tax information to other Federal agencies

[1] *Consumer Fraud and Identity Theft Complaint Data, January – December 2007*, FTC, dated February 2008; FTC's public Internet Web site, FTC.gov and Consumer.gov/sentinel.

with jurisdiction over certain non-tax criminal matters. The Treasury Inspector General for Tax Administration (TIGTA) believes the IRS should use these exceptions to the fullest extent possible in combating identity theft related to tax administration and work with the Office of the Assistant Secretary of the Treasury for Tax Policy to seek additional exceptions or clarify policy as needed.

Other systemic problems also hamper the IRS's ability to ensure the security of sensitive taxpayer information. For example, the IRS does not collect all transactions and audit trails[2] on its modernized systems, including the Customer Account Data Engine (CADE). This type of review is needed to determine whether IRS employees are illegally browsing through taxpayer files. While it may be understandable that legacy systems could not log these transactions due to older computer technology, there is no excuse for modernized systems not to have this capability.

Essentially, the IRS has failed to address these requirements during development of its modernized systems. As a result, it is deploying several new systems that lack detection capabilities. Without these audit trail logs, the IRS does not know what configuration changes are made or who makes them. Intruders and ill-intended IRS employees who have access to these components could steal taxpayer information with little chance of detection.

In addition, the IRS's Questionable Refund Program (QRP), which identifies and prevents fraudulent refund claims from being paid, has faced its own challenges. In May 2007, TIGTA reported that the IRS did not respond to various warning signs – including five previous TIGTA audit reports--that the QRP had problems and was becoming unmanageable.[3] In 2006, the IRS had quickly responded to a National Taxpayer Advocate's recommendation that certain changes be made to the QRP to restore a better balance between taxpayer rights and effective tax administration. However, some of those procedural changes may have adversely affected the IRS's ability to prevent potentially fraudulent refunds from being issued, possibly placing millions of dollars at risk. For example, TIGTA found that the use of criminal refund freezes, if implemented correctly and reviewed in a timely manner, could have prevented the issuance of over 20,000 fraudulent refunds totaling $71.7 million during Processing Year 2005.[4]

Overall, the IRS not only lacks the comprehensive data needed to determine the impact of identity theft on tax administration, it faces enormous challenges in securing the vast amount of personally identifiable taxpayer information that it stores.

---

[2] An audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.
[3] *Actions Have Been Taken to Address Deficiencies in the Questionable Refund Program; Many Concerns Remain, With Millions of Dollars at Risk* (Reference Number 2007-10-076, dated May 31, 2007).
[4] A processing year is the year in which tax returns and other tax data are processed by the IRS.

Security and Identity Theft

Each year, millions of taxpayers entrust the IRS with their sensitive financial and personal data that are stored in and processed by IRS computer systems. The risk that this sensitive data could be compromised and computer operations disrupted continues to increase. Both internal factors, such as the increased connectivity of computer systems and greater use of portable laptop computers, and external factors, such as the volatile threat environment related to increased phishing scams and hacker activity, contribute to these risks.

Phishing

Phishing is a deceptive practice by which an unsolicited e-mail directs unsuspecting victims to a fraudulent Web site that requests PII, such as credit card or bank account numbers, or other sensitive financial information. These scams continue to be a serious problem for the IRS.

The online phishing scam epidemic is growing exponentially. In Calendar Year 2007, an average of 2.46 host Web sites surfaced each day. That number has risen to 8.82 per day as of March 31, 2008 – a 359 percent increase over 2007.[5]

The IRS and TIGTA have coordinated efforts to thwart IRS-related phishing scams and minimize their impact on tax administration by leveraging the resources of both agencies. Since November 2005, TIGTA has identified phishing scams originating in 68 different countries. From March 2007 through February 2008, 1,418 phishing Web sites have been taken off the Internet. There has also been a dramatic increase in "Get Your Refund" phishing sites, and TIGTA anticipates that the economic stimulus payments this year will lead to new "Get Your Rebate" sites as well.

Although the volume of IRS-related phishing scams remains high, as of March 31, 2008, TIGTA has identified only seven phishing sites related to electronic tax return filing compared to 39 in all of 2007. These sites are designed to lure taxpayers into believing that they are filing their Federal income tax returns electronically with the IRS when, in fact, they are not. Criminals could be using different techniques this year that have not yet been identified, or they could be waiting until later in the filing season to establish the sites.

Insider attacks by employees and contractors continue to be a concern, because employees are more familiar with the IRS network than outsiders and can potentially do more harm. TIGTA's penetration tests on the IRS's internal network have shown that disgruntled employees and contractors could gain unauthorized access to employees' passwords and sensitive system data due to high-risk vulnerabilities, which are well-known to the hacker community. These vulnerabilities include blank and default passwords that system administrators failed to change when installing databases.

---

[5] Based on coordinated data tracking maintained by the TIGTA Strategic Enforcement Division and the IRS Computer Security Incident Response Center.

Personally Identifiable Information

Whether the attacks on security come from outside intruders or insiders, the target in the IRS is PII. TIGTA investigates individuals who attempt to steal PII and conducts proactive security assessments of IRS data systems to identify potential vulnerabilities that could be exploited by intruders. TIGTA also coordinates activities with the IRS Computer Security Incident Response Center (CSIRC) to reduce or eliminate any negative impact on tax administration by providing daily downloads to the CSIRC, informing the IRS of any potentially lost and/or stolen information technology assets.

The IRS stores PII for more than 130 million individual taxpayers who file annual Federal income tax returns. Each tax return includes the filer's name, address, Social Security Number, and other personal information. Approximately 30 percent of the tax returns also include the names and Social Security Numbers of at least one dependent. In addition, the IRS maintains PII on its employees and contractors.

The challenge of protecting this information from unauthorized disclosure is related not only to the volume of the data but also the complexity of ever-changing technology, which includes the IRS's more than 240 computer systems and 1,500 databases. Most of the IRS's approximately 100,000 employees and contractors have access to at least some of this information on a daily basis. Similar to recent news reports of breaches involving the improper browsing of presidential candidates' passport files, the IRS faces the risk of employees improperly accessing personal data contained in IRS computer systems.

To compound the risk that this information could be lost or stolen, some IRS employees regularly take laptop computers containing PII outside their offices to carry out their audit or collection duties and assignments. In March 2007, a TIGTA audit found that IRS employees reported the loss or theft of at least 490 computers and other sensitive data in 387 separate incidents.[6] Employees reported 296 (76 percent) of the incidents to TIGTA but not to the CSIRC. In addition, employees reported 91 of the incidents to the CSIRC; however, 49 of these were not reported to TIGTA.

The PII of at least 2,359 individuals in 126 of these incidents was lost. A test of 100 laptop computers used by IRS employees found that 44 of the computers contained unencrypted sensitive data, including taxpayer data and employee personnel data. Thus, it is likely that a large number of the lost computers contained similar unencrypted data. Employees did not follow encryption procedures because they were either unaware of security requirements or did so for their own convenience. As required by the Office of Management and Budget, the IRS has taken actions to encrypt data on all laptop computers, and TIGTA plans to determine the effectiveness of these corrective actions.

To address these challenges, security must become part of the fabric of the IRS. That is, all managers and employees must consider security ramifications along with

---

[6] *The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices* (Reference Number 2007-20-048, dated March 23, 2007).

productivity and quality concerns in their day-to-day activities. For years, however, IRS managers and employees have perceived security to be the responsibility of security professionals in the Modernization and Information Technology Services organization and the former Mission Assurance and Security Services organization. This cultural mindset limits the IRS's ability to strengthen overall security activities and controls within the organization and to provide assurance to the American taxpayers that their tax information is protected. While the IRS continues to remind executives that all managers and employees are responsible for the security of PII, TIGTA audit results reflect that managers and employees are not being held accountable for their lack of attention to their security responsibilities.

Weaknesses in two key areas – access controls and audit logs[7] – continue to plague the IRS.

Access Controls

In September 2007, TIGTA reported that managers continue to give employees access to systems they do not need to carry out their job responsibilities.[8] For example, systems administrators must be given total control over computer systems. Due to the sensitive nature of this position, the IRS must have proper controls in place to ensure that: 1) only appropriate employees have administrator rights and privileges; 2) administrator user accounts are reviewed annually for continued business needs; 3) user accounts are protected with strong passwords; and 4) user actions on computer systems are monitored for questionable activities. In the audit, covering five systems in several IRS offices, TIGTA could not find authorization and approval documentation for five percent of system administrator accounts (31of 607) for the five applications reviewed. Thirteen percent of active user accounts (79 of 607) were not needed because the employees no longer had a business need to administer their respective computer systems. In addition, weak passwords on user accounts existed on all five applications reviewed.

Because the IRS sends sensitive taxpayer and administrative information across its networks, routers on the networks must have sufficient security controls to detect and deter unauthorized use. TIGTA found that access controls for IRS routers were not adequate, and reviews to monitor security configuration changes were not conducted to identify inappropriate use. The IRS uses the terminal control system to administer and configure routers and switches, and users of this system must be authorized by managers. The IRS had authorized 374 accounts for employees and contractors that could be used to access routers and switches to perform system administration duties.

---

[7] Access controls limit access to systems and accounts to only authorized users. An audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.

[8] *Effectiveness of Access Controls Over System Administrator User Accounts Can Be Improved* (Reference Number 2007-20-161, dated September 19, 2007).

In March 2008, TIGTA reported that managers had not authorized 38 percent of the accounts (141of 374) used to administer key network components.[9] Over 84 percent of the configuration changes were made to the components using accounts shared by administrators so that accountability for the changes could not be established. Essentially, the IRS had no idea who had access to the network components.

Audit Trail Logs[10]

Because the IRS logs transactions on so few applications, it has no way to conduct the type of proper intrusion investigations that are needed to hold individuals accountable for unauthorized transactions and disclosures. The IRS has failed in prior attempts to provide a reasonable audit log process and does not expect to have one in place until 2014. This is an unacceptable major control weakness. The IRS cannot determine if, when, or where its sensitive data have been exposed.

Most notably, the IRS is not reviewing transactions on its modernized systems, including the CADE. The IRS could review limited audit trail information on the CADE, but it does not do so on a regular basis. In addition, some of the information and transactions on the CADE are not captured in an audit trail, thus, they cannot be reviewed. While it may be understandable that older legacy systems could not log transactions due to computer equipment available at the time, there is no excuse for modernized systems to not have this capability. Essentially, the IRS has failed to address these requirements during the development stages of its modernized systems. As a result, it is deploying new systems that lack detection capabilities. Any effort to install logging capabilities after deployment will likely cost significantly more than if the security capabilities had been designed into the systems during the system development phase.

TIGTA also raised concerns in the September 2007 report that audit trails were not being reviewed for four of the five applications tested. Although the IRS was capturing every key stroke from administrator user accounts and sending the data offsite for backup purposes for three of the four applications, it was not conducting required regular audit trail reviews. In a more recent audit, audit trail logs were not reviewed to monitor configuration changes. Without audit logs, the IRS did not know what configuration changes were being made or who made the changes. Intruders and malicious employees who had access to these components could steal taxpayer information with little chance of detection.

UNAX

Logging these transactions is vitally important because the Taxpayer Browsing Protection Act[11] mandates that the IRS identify and penalize employees who access

---

[9] *Inadequate Security Controls Over Routers and Switches Jeopardize Sensitive Taxpayer Information* (Reference Number 2008-20-071, dated March 26, 2008).

[10] An audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.

[11] Taxpayer Browsing Protection Act, Pub. L. No. 105-35, 111 Stat. 1104.

taxpayer accounts without authorization. The legacy computer system currently used to update taxpayers' accounts does, in fact, maintain an audit log enabling TIGTA to proactively identify IRS employees who commit unauthorized accesses (UNAX) of confidential taxpayer information.

TIGTA operates the UNAX detection program that identifies IRS employees who access taxpayer information without authorization. Whether the intent is fraud or simply curiosity, the potential exists for unauthorized accesses to tax information of high profile individuals and other taxpayers based on the volume of PII the IRS collects and stores. The competing goals of protecting this information and achieving workplace efficiencies become even more difficult as technology becomes faster and more complex.

For example, one recent prosecution involved an IRS employee who inspected the return information of a Certified Public Accountant (CPA) who had been preparing the former employee's tax returns for the past 30 years. The employee also inspected the tax returns and/or tax return information of approximately 56 clients of the CPA, a former employer, friends and relatives, and her friends' relatives. The employee was sentenced to four years of probation, six months of home confinement, and was fined $10,000.

Another IRS employee pleaded guilty to unauthorized access of a government computer. While an employee of the IRS, this individual accessed an IRS computer database containing taxpayer information and used a computer search function to search for taxpayers with the same first and last name as one of her relatives. The search resulted in a list of dozens of taxpayers with that name and also displayed the corresponding Social Security Number for each name. The employee provided the list to her relative, knowing that he intended to use the information to commit financial fraud through identity theft for private financial gain.

Since Fiscal Year 1998, the annual number of UNAX cases has increased from 430 to 521 in Fiscal Year 2007. Since Fiscal Year 1998, 471 employees have been removed, 452 have been suspended, and 934 have resigned for UNAX violations. In addition, since Fiscal Year 1998, TIGTA investigations have resulted in 185 prosecutions.

Sharing Federal Government Information

The IRS provides vast amounts of sensitive taxpayer data to U.S. Federal and State agencies and to contractors such as those associated with the IRS's Private Debt Collection initiative. TIGTA has evaluated the security of sensitive data at the private collection agencies during two audits. In March 2007, TIGTA reported several security weaknesses in the program but found that in Fiscal Year 2008 the two contractors had taken adequate corrective actions.[12] In particular, files were securely transmitted from the IRS to the contractors and adequately secured on the contractors' systems. Workstations

[12] *The Private Debt Collection Program Was Effectively Developed and Implemented, but Some Follow-up Actions Are Still Necessary* (Reference Number 2007-30-066, dated March 27, 2007); *Private Collection Agencies Adequately Protected Taxpayer Data* (Reference Number 2008-20-278, dated March 26, 2008).

used by contractor collection personnel were adequately controlled to prevent unauthorized copying of taxpayer information to removable media or transferring via e-mail. The contractors also maintained adequate audit trails and performed periodic reviews, including reviews to identify unauthorized access to taxpayer data. In addition, all contractors were subject to background investigations.

Identity Theft and Its Effect on Tax Administration

Recent reports of identity theft from both the private and public sectors have heightened awareness of the need to protect taxpayers' sensitive financial and personal data. There are two primary types of identity theft relating to tax administration:

- The first type involves an individual using another person's identity (name and Social Security Number) to file a fraudulent tax return to steal a tax refund. The individual committing this type of fraud frequently files the fictitious tax return electronically, early in the filing season.

  The individual whose identity was stolen later files his or her tax return and the IRS identifies it as a duplicate tax return. When this happens, the IRS freezes the second tax return, including any tax refunds due, and begins a process of corresponding with the individuals involved in the duplicate filing. This requires considerable time and effort by the legitimate taxpayer to prove he or she is a victim of identity theft. The victim's tax refund, if frozen, will not be issued until the matter is resolved.
- The second type involves using another person's identity (name, Social Security Number, or both) to obtain employment. This frequently involves undocumented workers. The wage information is reported to the Social Security Administration by the employer on the Wage and Tax Statement (Form W-2) under the stolen identification information (the victim's name and Social Security Number).

According to the FTC, 22 percent (56,125 of 258,427) of all reported identity theft complaints in Calendar Year 2007 resulted from either the filing of a fraudulent tax return or the misuse of someone's identity to obtain employment. This is up 10 percent from 2006. The FTC reports that the number of fraudulent tax returns filed as a result of identity theft increased 579 percent – from over 3,000 in Calendar Year 2002 to almost 21,000 in 2007.[13]

In July 2005, TIGTA reported that the IRS lacked a corporate strategy to adequately address identity theft issues.[14] In response to some of TIGTA's recommendations, the IRS agreed to develop: (1) updated agency-wide communication tools for educating and assisting taxpayers with information about identity theft; (2) agency-wide standards to ensure that the information taxpayers were asked to provide

---

[13] *Consumer Fraud and Identity Theft Complaint Data, January – December 2007*, FTC, dated February 2008; FTC's public Internet Web site, FTC.gov and Consumer.gov/sentinel.

[14] *A Corporate Strategy Is Key to Addressing the Growing Challenge of Identity Theft* (Reference Number 2005-40-106, dated July 22, 2005).

to substantiate identity theft claims is consistent throughout the IRS; (3) specific closing codes for cases involving identity theft that would allow the IRS to track and monitor the effect of identity theft on tax administration; and (4) processes to proactively identify instances of identity theft.

In October 2005, the IRS established the Identity Theft Program Office to provide centralized development of policy and procedural guidance within tax administration and to implement an agency-wide strategy composed of three components: outreach, prevention, and victim assistance. The Office was established in the Wage and Investment Division to facilitate cross-functional coordination. In 2007, the IRS moved the Identity Theft Program Office from the Wage and Investment Division to the Mission Assurance and Security Services (Mission Assurance) organization. According to the December 21, 2006, Memorandum of Understanding between Mission Assurance and the Wage and Investment Division, *". . . Identity Theft will be incorporated as part of enterprise information protection and will not be managed as a stand alone program office."* In July 2007, responsibility for the Identity Theft Program was assigned to the Deputy Commissioner for Operations Support. According to the IRS, ". . . reporting directly to a Deputy Commissioner will provide this program the ability to reach across all IRS organizations to ensure that proper attention and discipline is given . . ." to this important issue.

In March 2008, however, TIGTA reported that the IRS has not placed sufficient emphasis on employment-related and tax fraud identity theft strategies.[15] The IRS currently lacks the comprehensive data needed to determine the impact of identity theft on tax administration. Its prevention strategy does not include pursuing individuals using another person's identity, unless a given case directly relates to a substantive tax or conspiracy violation. According to IRS policy, the actual crime of identity theft will only be investigated by its Criminal Investigation Division if the crime is committed in conjunction with other criminal offenses having a large tax effect. In Fiscal Years 2005 and 2006, the IRS recommended only 45 and 55 cases, respectively, for prosecution that included charges of identity theft.

Due to the IRS's lack of information related to identity theft, it is not clear whether the IRS Criminal Investigation Division evaluated or investigated any of these complaints. According to the IRS, the Criminal Investigation Division does not use FTC Identity Theft Clearinghouse data.[16]

In addition, actions taken in response to employment-related identity theft are not adequate to stop the unlawful use of the identity. Although the Social Security Administration notifies employers of mismatches between names and Social Security Numbers, the IRS does not notify them when their employees are using someone else's

---

[15] *Outreach Has Improved, but More Action Is Needed to Effectively Address Employment-Related and Tax Fraud Identity Theft* (Reference Number 2008-40-086, dated March 25, 2008).

[16] The Identity Theft Clearinghouse is the sole national repository of consumer complaints about identity theft. The database is maintained on the FTC Consumer Sentinel Network, a secure, encrypted Web site for use by law enforcement agencies.

identity. Social Security Number/name mismatches are indeed a significant problem for the IRS and the Social Security Administration; however, a more serious problem develops for the lawful taxpayers when both their names and Social Security Numbers are used by others to gain employment. Because the IRS and the Social Security Administration assume that the information on the *Employee's Withholding Certificate* (Form W-2) is accurate, the earnings resulting from the identity theft will be attributed to the lawful taxpayers for determining both Social Security benefits and tax liabilities.

IRS officials explained that the Internal Revenue Code confidentiality and disclosure provisions prevent the agency from taking actions to stop continued use of another person's identity for employment, and that it is broadly restricted from sharing taxpayer information with third parties. The IRS also does not pursue the taxes that might be due on income earned using a stolen identity because it does not have sufficient enforcement resources to address most of the identity theft cases.

Additionally, the IRS does not believe that it is worthwhile to pursue employment-related identity theft cases for unreported tax liabilities because the taxes owed on most of these cases are not significant. TIGTA is concerned that if the IRS takes no additional action to address the misreporting of income resulting from identity theft, there is no deterrent to keep the problem from spreading.

Use of another person's identity for employment results in the misreporting of income which affects income tax and Social Security tax as well as other employment taxes. Agencies with jurisdiction over these matters include the IRS and the Social Security Administration. Consequently, coordination between these agencies is important to ensure that Federal records related to income earned by a taxpayer are correct and to ensure appropriate law enforcement. Federal law[17] allows the Social Security Administration to pursue criminal penalties for an individual who fraudulently obtains, uses, or represents a Social Security Number to be theirs. There are exceptions in the Internal Revenue Code that allow disclosure of tax information to other Federal agencies with jurisdiction over certain non-tax criminal matters. If the IRS believes these exceptions are not adequate for the purposes of combating identity theft, IRS management should seek legislative remedy through the Office of the Assistant Secretary of the Treasury for Tax Policy. The IRS provided a copy of TIGTA's report to the Office of the Assistant Secretary of the Treasury for Tax Policy to evaluate whether a legislative remedy should be sought for this issue.

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

---

[17] 42 U.S.C. § 408 provides for criminal penalties for an individual who fraudulently buys, sells, or possesses a Social Security card with intent to sell or alter or who discloses, uses, or compels the disclosure of the Social Security Number of any person in violation of the laws of the United States.

- The Automated Underreporter function contacted taxpayers multiple times for the same compliance issues even though these taxpayers' cases were previously marked as closed for identity theft. The Automated Underreporter function is a compliance function using third-party information returns to identify income and deductions that were not reported on tax returns.[18]
- The Withholding Compliance function unnecessarily contacted taxpayers for withholding issues because the function does not consider the Identity Theft Closing codes used by the Automated Underreporter function's computer system. The Withholding Compliance function ensures that taxpayers who have serious under-withholding problems are brought into compliance with Federal income tax withholding requirements. The function uses Form W-2 information to identify taxpayers with insufficient withholding and attempts to correct withholding to ensure that taxpayers have enough income tax withheld to meet their tax obligations.

In January 2008, the IRS implemented the universal identity theft indicator. The effective use of this universal identity theft indicator should reduce the number of multiple contacts made with taxpayers who have been victims of identity theft. Once a taxpayer has been coded as an identity theft victim, he or she should no longer be selected and contacted by the various IRS functions for compliance issues that resulted from the identity theft.

The IRS advised TIGTA that it is implementing a five-year strategy for its Privacy, Information Protection, and Data Security Office that will include identity theft issues. However, it did not state when this strategy will be implemented, what milestones will be established, and how its success will be measured.

The IRS has also indicated that it is collaborating with the FTC on outreach activities. It is also using extracts of general information from the Identity Theft Clearinghouse to track trends and develop process improvements and outreach initiatives for victim assistance. Yet, the IRS has concluded that the FTC data are not useful in evaluating or investigating tax fraud or employment-related identity theft, even though the Identity Theft Clearinghouse is the sole national repository of consumer identity theft complaints and should be an important source of data for the Criminal Investigation Division.

Identity Theft and the Questionable Refund Program

The QRP, which was established to identify and prevent the issuance of fraudulent refunds, received harsh criticism from the National Taxpayer Advocate as a program that was inefficient, ineffective, and did not afford taxpayers their rights. In 2006, the IRS re-evaluated its processes and procedures to address the Taxpayer

[18] The annual underreporter process begins when the IRS creates an inventory list of potential underreporter cases by matching taxpayer return data against the data in the third-party information return database, identifying taxpayers with discrepancies. The first match occurs between July and September of each year; a second match, picking up additional filers, occurs during January and February of each year.

Advocate's concerns. Yet, TIGTA believed that several of these changes might adversely affect the IRS's ability to prevent the issuance of millions of dollars in potentially fraudulent refunds.

The Growing Problem of Identity Theft and Tax Return Fraud

Of the 44,788 tax refunds verified as fraudulent by the IRS's QRP through September of Processing Year 2006, the Criminal Investigation Division indicated that approximately 18 percent involved identity theft.[19] However, the QRP processing changes made in 2006 could have resulted in a burden on the victims of identity theft, lost revenue, and additional IRS resources to resolve these accounts.

The IRS's policy prior to Processing Year 2006 was to freeze both the current and future years' tax accounts when the QRP found fraud. This automatically prevented the issuance of any refunds to these taxpayers for their current and subsequent tax years, including identify theft victims. The 2005 National Taxpayer Advocate's Report highlighted the automatic freezing of future years' refund returns as a significant problem with the QRP because it caused significant and continuing inconvenience to identity theft victims whose refund returns in those future years were legitimate.[20] As a result of the Advocate's report, the IRS decided in 2006 to discontinue freezing the future years' accounts when fraud is found.

TIGTA reported a concern with this revised procedure because the future year freeze was an effective means for protecting revenue, when considered along with other changes that included notifying taxpayers that their refunds had been frozen and minimizing the time that refunds are frozen. These additional changes minimized the burden on taxpayers and allowed the IRS to systemically protect the government's revenue. A sample of fraudulent refund returns filed during Processing Year 2004 identified that 42 percent of those accounts had a repeat incident of refund fraud the following year.

In a March 2008 congressional statement, the National Taxpayer Advocate described that in a typical identity theft refund fraud situation, the perpetrator submits a fraudulent tax return early in the filing season using the personal information of an innocent taxpayer before the actual owner of the Social Security Number has an opportunity to file a legitimate tax return. Because the IRS does not know that this is a return involving identity theft, any refund due is issued to the perpetrator. When the identity theft victim later attempts to file his or her tax return, the IRS flags it as a duplicate return and prevents any refund claimed on the true return from being issued.[21]

---

[19] *Actions Have Been Taken to Address Deficiencies in the Questionable Refund Program; Many Concerns Remain, With Millions of Dollars at Risk* (Reference Number 2007-10-076, dated May 31, 2007).
[20] *National Taxpayer Advocate's 2005 Annual Report to Congress* (Publication 2104, Rev. 12-2005).
[21] Written Statement of Nina E. Olson, National Taxpayer Advocate, before the Subcommittee on Oversight Committee on Ways and Means, U.S. House of Representatives Hearing on: The 2008 Tax Return Filing Season, IRS Operations, FY 2009 Budget Proposals, and The National Taxpayer Advocate's 2007 Annual Report to Congress (March 13, 2008).

When this occurs, the identity theft victim will likely contact the IRS to ask what happened to his or her refund.

This contact would have also likely occurred if the IRS had frozen the subsequent year account of a prior identity theft victim. The identity theft victim would contact the IRS asking about his or her refund that had been frozen. However, the advantage of having the refund already frozen is that it allows the IRS to identify these cases upfront. It can then be proactive through a timely determination of whether the taxpayer is again the victim of identity theft – or if the refund is valid – and notifying the victim of a delay in receiving his or her refund.

With the high risk of repeat problems for innocent taxpayers, a future year automatic freeze on at least one subsequent tax return might help reduce the adverse effects of identity theft by allowing the IRS a brief window of time to prevent a fraudulent tax return from being processed. If the Criminal Investigation Division properly identifies identity theft freezes, notifies the taxpayers of the freezes, and resolves the freezes in a timely manner, the IRS will be providing a valuable service to innocent taxpayers, while also protecting Federal revenue and minimizing taxpayer burden if the return does not involve a repeat occurrence of identity theft.

The Role of the Questionable Refund Program in Identifying and Preventing Fraud

The IRS relies on the QRP to identify and prevent fraudulent refund claims from being paid. Over the past several years, TIGTA has reported that the QRP was becoming increasingly unmanageable due to the growing number of fraudulent claims and the IRS's lack of resources to combat the fraud.[22] In addition, the QRP was severely curtailed when the IRS and its information technology contractors failed to launch a Web-based version of its primary information system, the Electronic Fraud Detection System, during Processing Year 2006. Unfortunately, this resulted in dramatic decreases in the amount of refund fraud the IRS identified and stopped that year. For Processing Years 2007 and 2008, the IRS reverted to a legacy version of the Electronic Fraud Detection System.

In May 2007, TIGTA reported that the IRS did not respond to various warning signs, including five previous audit reports, that the QRP was facing problems and becoming unmanageable.[23] Nevertheless, the IRS quickly responded to the National Taxpayer Advocate's Report and made changes to the QRP in Processing Year 2006 that were intended to address the Advocate's concerns and reduce the burden on taxpayers. While TIGTA is encouraged by the IRS's actions to address stakeholder concerns and restore balance between taxpayer rights and effective administration of the tax laws, some procedural changes may have adversely affected the IRS's ability to prevent potentially fraudulent refunds from being issued in the future, possibly placing millions of dollars at risk. For example, TIGTA found that the use of criminal refund freezes, if

---

[22] *The Internal Revenue Service Needs to Do More to Stop the Millions of Dollars in Fraudulent Refunds Paid to Prisoners* (Reference Number 2005-10-164, dated September 28, 2005).
[23] *Actions Have Been Taken to Address Deficiencies in the Questionable Refund Program; Many Concerns Remain, With Millions of Dollars at Risk* (Reference Number 2007-10-076, dated May 31, 2007).

implemented correctly and reviewed in a timely manner, could have prevented the issuance of over 20,000 fraudulent refunds totaling $71.7 million during Processing Year 2005.

Additionally, the IRS needed to be more aggressive in adjusting accounts with frozen refunds to either recover fraudulent refunds that were issued or to prevent repeat fraud. TIGTA estimated that had the IRS taken action on earlier fraudulent returns, it could have prevented $27.5 million of future potentially fraudulent refunds.

Identifying prisoner refund fraud continues to be a problem. In the 2007 report, TIGTA found that only 4,235 prisoner returns claiming approximately $19 million in refunds were identified as fraudulent in Processing Year 2006 and only $11.5 million in refunds were stopped. In contrast, during Processing Year 2004, 18,159 prisoner returns claiming $68.2 million in fraudulent refunds were identified and 14,033 refunds totaling $53.5 million were stopped. This indicates the potential magnitude of the IRS's lost ability to detect and stop fraudulent prisoner refunds during Processing Year 2006 when the Electronic Fraud Detection System was not available.

Understandably, the IRS made processing decisions in the context of balancing available resources with workload, but concerns remain that those decisions could have a negative impact on effective tax administration. Continuing to freeze the subsequent year's return, when properly controlled, is an efficient and effective means of identifying repeat fraud, protecting revenue, and protecting innocent taxpayers who are victims of identity theft. The IRS has continued to advise us that it does not have sufficient resources to effectively and promptly deal with a rapidly growing fraudulent refund problem. Recognizing the challenge of limited resources, TIGTA recommended that the Criminal Investigation Division take a leading role in pursuing legislation that would change current legal procedures that would allow the IRS to reverse fraudulent tax return information. This would streamline account resolutions while still protecting taxpayer rights.

TIGTA has an ongoing audit focused on the QRP to evaluate the impact of the failure of the Electronic Fraud Detection System on the IRS's ability to identify and stop questionable refunds during Processing Year 2006 (for example, the amount of fraudulent refunds that were issued) and to determine the effectiveness of the IRS's QRP processes during Processing Year 2007. Among other issues, the current audit will also estimate the impact that the higher dollar threshold had on stopping fraudulent refunds during Processing Year 2007. The IRS advised TIGTA that the need to implement thresholds to exclude tax returns occurred because of limited IRS resources available to process fraudulent tax returns identified through the QRP.

The IRS was more successful in stopping fraudulent refund claims during Processing Year 2007 than in past years. According to the IRS Criminal Investigation Division, over $1.2 billion in fraudulent tax refunds were stopped during Processing Year 2007. This amount represents a 152 percent increase over Processing Year 2005. Also, according to Division data, the QRP became more effective in stopping fraudulent refund

claims because only those returns with the highest potential for fraud were verified. TIGTA will continue to monitor this very important area as the IRS seeks additional solutions to combat the rapidly growing problem of fraudulent tax refunds.

2008 Filing Season

The 2008 Filing Season appears to be progressing without major problems. As of March 29, 2008, the IRS reported it had received approximately 86.8 million tax returns. Of those, approximately 62.2 million were filed electronically (e-filed) (an increase of 9.3 percent from this time in 2007), and approximately 24.6 million were filed on paper (an increase of 4.8 percent from this time in 2007). Additionally, nearly 69.8 million refunds totaling approximately $172 billion had been issued. Of these, 50.8 million (73 percent of all refunds) were directly deposited to taxpayer bank accounts, an increase of 7.3 percent compared to 2007.

Use of the IRS's free online filing program had been declining in prior years. However, based on the current volume, it appears that taxpayers are increasingly taking advantage of this option; the number has increased by 17.4 percent from 2007. Additionally, the number of taxpayers who e-file from their home computers has increased by 17.3 percent this filing season.

Due to late passage of the Tax Increase Prevention Act of 2007,[24] which provides relief to taxpayers who would have been subject to the Alternative Minimum Tax, five tax forms that were affected by the legislation could not be processed until February 11, 2008. The February 11 date allowed the IRS enough time to update and test its systems without major disruptions to other return processing operations. The week ending February 15, 2008, was the first week for processing returns with the five affected forms. As a result, receipts increased by 20.9 percent over the same week last year. TIGTA is evaluating the effect on taxpayers of the delay in processing the five tax forms related to the Alternative Minimum Tax legislation.

The latest release of the CADE, Release 3.0, was originally developed to deliver 17 new functions and capabilities. The IRS divided Release 3.0 into two sub-releases. CADE Release 3.1 contained four major functions and was deployed between August and October 2007. CADE Release 3.2 included seven major functions and was delivered in February 2008. The major functions delivered include the capability of processing tax returns with a disaster area designator; processing tax returns claiming the Earned Income Tax Credit, Credit for Child and Dependent Care, and requests for Split Refunds; providing address change service requests; and validating tax balances. The remaining six functions will be determined for delivery in future releases of the CADE. These additional capabilities were expected to significantly increase the volume of returns posting to the CADE from the approximately 11.2 million returns posted during Calendar Year 2007. As of March 28, 2008, about 21.1 million tax returns had been posted to the CADE.[25]

---

[24] Tax Increase Prevention Act of 2007, Pub. L. No. 110-166 Stat 2461 (2007).
[25] TIGTA has not evaluated the accuracy of the postings.

Economic Stimulus Act of 2008[26]

In keeping with the intent of the Economic Stimulus Act of 2008, the IRS expects to issue over $100 billion in stimulus payments (often referred to as rebates) and is trying to ensure that everyone who is entitled to the rebates knows what to do to receive it. The IRS sent Economic Stimulus Payment Notices (Notice 1377) to more than 130 million taxpayers who filed a Tax Year 2006 income tax return. These notices were mailed from March 4 to March 21, 2008, and cost an estimated $45 million to print and mail. The notice was informational only and did not require a response from the taxpayer. Beginning in May 2008, an additional notice will be mailed to those taxpayers eligible for the payments to explain the payment amount and how it was calculated. The IRS believes it will receive significantly fewer calls to its toll-free telephone information line as a result of issuing these notices.[27]

The IRS also created a new tax package *Information About Economic Stimulus Payments for Social Security, Veterans, and Other Beneficiaries* (Package 1040A-3) to be mailed to more than 20 million individuals who normally do not have to file tax returns but might qualify for the stimulus payments (for example, those who receive Social Security Administration and Department of Veterans Affairs benefits). The law provides for payments to these individuals if they have a total of $3,000 or more in qualifying income. Qualifying income is earned income, certain Social Security Administration, Railroad Retirement, and Department of Veterans Affairs benefits, and non-taxable combat pay.

As of March 28, 2008, the IRS had received an estimated 1.4 million tax returns from individuals who filed them solely to receive the rebates. Since these are tax returns that would normally not have to be filed, the normal IRS refund controls are not geared for this situation. The IRS is evaluating alternatives to identify any of these tax returns that are fraudulent so it can prevent any associated fraudulent stimulus payments. TIGTA is currently evaluating the controls over the processing of these tax returns and monitoring their volume and effect on the 2008 Filing Season.

Since the Economic Stimulus Act of 2008 was enacted, the IRS has been averaging more than 63,000 calls per day beyond the normal volume to its toll-free telephone lines related to the upcoming rebates. However, for the one week ending March 29, 2008, the IRS averaged more than 144,000 calls per day to its toll-free telephone lines related to the rebates. At peak, the IRS plans to use 1,067 Automated Collection System[28] telephone assistors to take rebate telephone calls during their regular tours of duty and has also trained more than 500 tax examiners and assistors (who

---

[26] Economic Stimulus Act of 2008, Pub. L. No. 110-185 (2008).

[27] The IRS estimates one telephone contact with an IRS assistor costs almost $20. Mailing one stimulus payment notice costs approximately 35 cents.

[28] The Automated Collection System is an integral part of the IRS process for collecting unpaid taxes and securing unfiled tax returns from both individual and business taxpayers. When taxpayers do not comply with the IRS's computer-generated notices, Automated Collection System tax examiners attempt to contact them by telephone to secure payments or unfiled returns. The Automated Collection System is the computer system that assigns these cases to the individual tax examiners.

normally work taxpayer correspondence and paper casework) to answer general rebate calls. Additionally, 2,100 Automated Collection System assistors will be offered the opportunity to work weekday overtime on an "as needed" basis. The IRS will also utilize overtime and extend the employment of its seasonal hires.

The IRS stopped the issuance of Automated Collection System enforcement tools (systemic notices and letters were stopped on February 22 and systemic levies on February 29). Issuance of regular delinquency notices on accounts not yet assigned to the Automated Collection System has not been stopped, and the IRS expects to reserve 40 percent to 50 percent of the available Automated Collection System staff to answer calls from taxpayers who respond to these notices. The IRS plans to restart the notices when telephone demand decreases. The IRS reports that the foregone revenue associated with these actions could be as high as $666 million.

TIGTA is reviewing the IRS's planning and preparation for issuing the stimulus payments. TIGTA will continue to closely monitor the issuance of the payments and their effect on customer service and enforcement activities. Future reviews are planned on the accuracy of the payments, costs of distribution, and effects the payments might have, if any, on Tax Year 2008 tax returns and the 2009 Filing Season.

Providing Quality Customer Service

Providing quality customer service to the American taxpayer will always be a challenge for the IRS. Nevertheless, it has made consistent progress. In April 2007, the IRS issued the Taxpayer Assistance Blueprint Phase 2 report, which presents the IRS's guiding principles and Strategic Plan for taxpayer services. The Strategic Plan includes performance measures, service improvement portfolios, and an implementation strategy.

IRS.gov

IRS.gov continues to be one of the most visited Web sites in the world, especially during filing seasons. As of March 22, 2008, the IRS reported more than 111 million visits to IRS.gov, a 16.7 percent increase over last year. Almost 25 million taxpayers went to IRS.gov to obtain their refund information via the "Where's My Refund?" option, a 20.2 percent increase over last year.

Taxpayer Assistance Centers

Taxpayer Assistance Centers are walk-in sites where taxpayers can receive answers to account and tax law questions, as well as assistance in preparing their tax returns. As of March 22, 2008, the Centers had served approximately 1.8 million taxpayers this filing season.

In Fiscal Year 2007, the IRS implemented a standardized quality measurement system to measure the quality of taxpayer service at the Centers. As of March 22, 2008,

the IRS had reported a 59 percent accuracy rate for tax law questions and an 83 percent accuracy rate for tax account questions for this fiscal year.

Toll-Free Operations

The IRS expects increased demand this year for its toll-free telephone assistance lines related to the upcoming stimulus payments. However, all planning for the 2008 Filing Season was completed before the economic stimulus legislation was passed, and calls related to the upcoming rebates have affected service. The IRS had planned to provide an 82 percent Level of Service for Fiscal Year 2008, but has projected the Level of Service could be as low as 74 percent. The Level of Service is the primary measure of service to taxpayers. It is the relative success rate of taxpayers who call for services on the IRS toll-free telephone lines.

For the 2008 Filing Season (as of March 29, 2008), the IRS had already answered about 112 percent of the planned 10.9 million assistor-answered calls. Its 80.0 percent Level of Service is 4.5 points lower than the actual 2007 Filing Season Level of Service of 84.5 percent. Additionally, the IRS had planned to answer 14.8 million automated calls but had answered 16.1 million automated calls.

The IRS expects to receive approximately 1.8 million calls from March through April 2008 related to rebates and additional calls in May through July after the IRS mails detailed notices to taxpayers. To ensure that taxpayers are able to call the toll-free lines, the IRS states that it is maximizing availability of the telephone lines and the assistors. In late January 2008, the IRS began receiving higher volumes of calls from taxpayers inquiring about the stimulus payments. To reduce the demand on assistors, the IRS implemented an automated message on the 1-800-829-1040 and 1-800-829-4933 toll-free telephone lines. On February 19, 2008, the IRS dedicated a separate telephone line (Rebate Hotline) to the automated message on the rebates. From the end of January through March 29, 2008, the IRS has received 2.2 million calls to all automated rebate lines. In addition to the 2.2 million automated calls, IRS assistors have answered 572,000 calls about the stimulus payments.

The IRS has also extended its toll-free telephone service by opening it on March 29, 2008, for Super Saturday. Super Saturday is the day the IRS opened 320 Taxpayer Assistance Centers to help reach Americans who are eligible for the stimulus payments, but who normally are not required to file income tax returns. The IRS opened the toll-free Rebate Hotline on Super Saturday between 9 a.m. and 3 p.m. local time.

Volunteer Program

Each year, more taxpayers choose to have volunteers prepare their tax returns. So far this filing season, almost two million tax returns have been prepared by volunteers, an increase of 17 percent over the 2007 Filing Season. The IRS's Volunteer Program is playing an increasingly important role in the IRS's efforts to improve taxpayer service

and facilitate participation in the tax system. The Program provides no-cost Federal tax return preparation and electronic filing to underserved taxpayer segments, including low-income, elderly, disabled, and limited-English-proficient taxpayers. These taxpayers are frequently involved in complex family situations that increase the difficulty of correctly understanding and applying tax laws.

During this filing season, TIGTA auditors are visiting 36 Volunteer Income Tax Assistance and Tax Counseling for the Elderly sites across the United States. The auditors pose as taxpayers to determine whether taxpayers are receiving quality service, including the accurate preparation of their individual income tax returns. Auditors developed scenarios designed to test quality controls and present volunteers with a wide range of tax law topics that taxpayers may need assistance with when preparing their tax returns. These scenarios include the characteristics (for example, income level, credits claimed) of tax returns typically prepared by Volunteer Program volunteers based on an analysis of the Tax Year 2007 volunteer-prepared tax returns.

As of March 28, 2008, 30 tax returns had been prepared with a 67 percent accuracy rate, which is an increase over the 56 percent accuracy rate TIGTA reported for the 2007 Filing Season. Volunteers are doing a better job of using the tax tools and information available when preparing tax returns.

Paid Preparers

Paid preparers are an important source in assisting taxpayers in filing their tax returns on time, paying their taxes, and receiving refunds. During this filing season, TIGTA conducted an audit to determine whether taxpayers receive accurate preparation of their income tax returns when using commercial chain preparers and unenrolled paid preparers.[29] In Tax Year 2006, paid preparers prepared over 85 million individual Federal income tax returns, which was a 9 percent increase above the nearly 78 million tax returns prepared by paid preparers in Tax Year 2005. Currently, there are no national standards that a preparer is required to satisfy before selling tax preparation services to the public. Anyone – regardless of training, experience, skill, or knowledge – may prepare Federal income tax returns for others for a fee.

Paid preparers who are authorized to represent taxpayers in matters before the IRS are called practitioners. They include attorneys, CPAs, enrolled agents, and actuaries. These practitioners, who can legally represent taxpayers, serve as a conduit to the IRS on account-related matters and are regulated by the IRS Office of Professional Responsibility.

All paid preparers are subject to Internal Revenue Code penalties – both civil and criminal. For example, civil penalties apply if paid preparers do not sign the tax returns they prepare, do not provide the taxpayers with copies of the tax returns, or deliberately understate a taxpayer's tax liability. Criminal penalties apply when a paid preparer

[29] Accuracy of Tax Returns Prepared by Unenrolled Paid Preparers (Audit Number 200840009).

willfully prepares or makes a false statement regarding a false or fraudulent tax return or knowingly provides fraudulent tax returns to the IRS.

In February and March 2008, TIGTA auditors posed as taxpayers in one large metropolitan area and had 27 tax returns prepared by individuals employed at both commercial chains and small independently owned tax preparation offices. The tax returns were not filed. Auditors explained to preparers that they would file the tax returns themselves.

Auditors used five scenarios with income ranging from $16,000 to $85,000. One scenario had self-employment income. The filing statuses ranged from Single or Married Filing Jointly to Head of Household. The issues included, for example, dependency exemptions, child care expenses, early withdrawal from a retirement plan, the Earned Income Tax Credit, and business expenses. TIGTA also used two of these scenarios in its filing season review of the Volunteer Program.

In its visits to tax preparation offices, TIGTA found that only 41 percent (11 of 27) of tax returns were considered to be prepared accurately. Among the inaccuracies, TIGTA found:

- 11 of 27 tax returns contained mistakes and omissions believed to be caused by human error and/or the complexity of the tax laws; and
- 5 of 27 tax returns contained misstatements and omissions that significantly affected the tax liability believed to be caused by willful or reckless conduct.

For six tax returns prepared inaccurately, taxpayers would have received unjustifiable refunds of $6,318. In 10 instances, taxpayers would have owed taxes of $6,472. In one case, a correctly prepared tax return would have resulted in a refund of $98, but instead resulted in a balance due of more than $6,000.

Refund Anticipation Loans

During the 2008 Filing Season, TIGTA also conducted an audit to determine the impact of Refund Anticipation Loans (RAL) on taxpayers and tax administration.[30] A RAL is a short-term loan based on a taxpayer's expected income tax refund and is a contract between the taxpayer and a lender. The lender is a bank and the facilitator is usually the tax preparer or tax preparation company. The bank first deducts fees for tax return preparation, e-filing, finance charges, and processing. The taxpayer receives the balance of the refund by check, direct deposit, debit card, or as a down payment on a good or service. Once the IRS processes the tax return that generated the refund, the IRS transfers the funds directly to the bank to repay the loan. The IRS is not involved in the contract, cannot grant or deny the loan, and cannot answer any questions about it.

As of March 28, 2008, approximately 18.6 million taxpayer accounts for Tax Year 2007 included RAL indicators. This includes 10 million taxpayers who filed tax

[30] Assessment of Refund Anticipation Loans (Audit Number 200840012).

returns claiming the Earned Income Tax Credit.[31] The IRS explained that preparers input the RAL indicator on the accounts when taxpayers apply for the loans.

As part of the audit, TIGTA conducted a telephone survey of 350 taxpayers whose Tax Year 2007 accounts contained RAL indicators. The survey was designed to gain an understanding of why taxpayers obtain RALs and determine the taxpayers' experiences during the process and the cost of the loans.

Of the 350 taxpayers surveyed, 81 percent (284) stated that they were unaware of IRS's free tax return preparation services for which they qualified. Seventy-one percent of respondents (250) stated that they had actually received RALs. The other 29 percent (100) did not apply for a RAL, applied but did not obtain the loan, or received a Refund Anticipation Check. A Refund Anticipation Check is a non-loan alternative to RALs. With a Refund Anticipation Check, the bank sets up a temporary account to receive the refund. Once the refund is deposited into this account, the bank deducts return preparation, filing, and bank processing fees before disbursing the remainder of the funds to the taxpayer.

Of the 250 respondents who stated that they had received RALs, 85 percent (213) stated that they understood they were receiving loans and that their preparers explained the fees – although most could not tell auditors the annual percentage rate they were charged for the loans.

Eighty-five percent (213) of respondents stated that they obtained the loans to more quickly receive their refunds and most used the funds to pay bills. About one-half received their loans within two business days. Additionally, 64 percent (159) stated that they had a checking or savings account in a financial institution.

IRS records show that some respondents who stated they did not receive a RAL might have received one, while other respondents who stated they received a RAL might not have received one. TIGTA is conducting additional research to resolve the discrepancies, as well as analyzing, for example, the amount of time it took the refunds to be deposited into the banks, whether the tax returns were posted on the CADE, and whether there were debt indicators or freezes on the respondents' accounts. In addition, selected demographics will be identified and analyzed.

Conclusion

Overall, the 2008 Filing Season appears to be progressing without major problems. The IRS has taken positive actions to prepare for the issuing of over $100 billion in stimulus payments beginning in May. In addition, the IRS has improved its quality customer service by creating a strategic plan to focus on service improvement and performance measures.

---

[31] The Earned Income Tax Credit is a refundable Federal tax credit for low-income working individuals and families.

However, TIGTA is concerned about the proliferation of phishing scams that attempt to trick taxpayers into providing sensitive tax information. Insider attacks by IRS employees and contractors continue to be a concern. Because of their familiarity with the IRS network, they can potentially do more harm than outsiders. Whether the attacks come from outside intruders or inside the IRS, the target is personal and financial information. While the IRS relies on its QRP to identify fraudulent refund claims and prevent them from being paid, TIGTA is concerned that the QRP is becoming increasingly unmanageable due to the growing number of fraudulent claims and the IRS's lack of resources to combat the fraud.

Furthermore, the IRS has placed only limited emphasis on employment-related and tax fraud identity theft. Although the Internal Revenue Code currently permits the referral of tax information to certain Federal law enforcement agencies, the IRS does not appear to be fully utilizing this authority. The IRS Criminal Investigation Division investigates identity theft crimes only if they are committed in conjunction with other criminal offenses having a large tax effect. As a result, the IRS has mainly focused on combating identity theft through public outreach. In addition, current processes have been inadequate in reducing burden for taxpayers victimized by identity theft. The IRS still lacks the comprehensive data needed to determine the impact identity theft is having on tax administration.

I hope that my discussion of tax-related identity theft and the 2008 Filing Season will assist you with your oversight of the IRS. Mr. Chairman and Members of the Committee, thank you for the opportunity to share my views.

United States Senate Committee on Finance Hearing
Identity Theft: Who's Got Your Number?
April 10, 2008

Questions Submitted for the Record

Questions for Mr. George:

Chairman Baucus

1. **TIGTA has completed several studies assessing the IRS's ability to detect and deal with identity theft and to protect taxpayer information. Many of TIGTA's reports have been critical of the IRS. A recent report concludes, "The IRS has not placed sufficient emphasis on employment-related and tax fraud identity theft strategies."**

    a. **Why has the IRS failed to develop an effective agency-wide identity theft strategy?**

RESPONSE:

The efforts of IRS officials responsible for identity theft have been too limited in scope. Recognizing this, the IRS has reorganized and shifted responsibility for the program a number of times, but with limited effect.

The IRS established the Identity Theft Program Office (Program Office) in October 2005 to provide centralized development of policy and procedural guidance within tax administration and to implement an agency-wide strategy. The Program Office was a small component within the Wage and Investment Division, and did not effectively facilitate cross-functional coordination. The Program Office consisted only of a Program Chief and three staff members, and their efforts predominantly focused on public outreach and education. In September 2006, the Identity Theft Program was transferred from the Wage and Investment Division to the Mission Assurance and Security Services function. By May 2007, the new Program Office was not yet fully staffed. Then in July 2007, responsibility for the Identity Theft Program was assigned to the Deputy Commissioner for Operations Support.

Moreover, the IRS does not appear to be willing to devote resources to pursue individuals who are using another person's identity. The IRS Enterprise Identity Theft Strategy does not include pursuing individuals using another person's identity, unless their cases directly relate to tax fraud. Employment-related fraud cases worked by the Criminal Investigation Division address employment tax issues but do not address the illegal use of Social Security Numbers (SSNs) for employment. The Criminal Investigation Division investigates the actual crime of identity theft only if it was committed in conjunction with another criminal offense having a large tax effect.

b. To what extent has the IRS followed TIGTA's recommendations regarding its identity theft strategy? Describe TIGTA's follow-up effort to determine to what extent the recommendations have been followed.

RESPONSE:

The IRS has made some progress in implementing TIGTA's recommendations, especially in the areas of outreach and victim assistance. The IRS has not made much progress in reducing tax fraud or employment-related identity theft.

In 2005, we reported[1] that the IRS lacked a corporate strategy to adequately address identity theft issues. The IRS agreed to:

1. Update agency-wide communication tools to educate and assist taxpayers with information about identity theft.
2. Issue agency-wide standards so that information requested of taxpayers to substantiate identity theft claims is consistent throughout the IRS.
3. Develop specific closing codes for cases involving identity theft to allow the IRS to monitor the effect of identity theft on tax administration.
4. Follow through on the Identity Theft Task Force's goal of developing an Enterprise Identity Theft Strategy, to include processes to proactively identify identity theft, resolve identification number discrepancies, and ensure appropriate tax withholding.

Specifically, the IRS said it would work with employers through several initiatives to reduce the incidence of employment-related identity theft, and that tax return preparers who promote schemes for clients to make false claims of identity theft to underreport income and maximize refundable credits would face penalties and sanctions.

TIGTA performed a follow-up review in 2007. We found that the Identity Theft Program Office has focused mostly on its Enterprise Strategy for public outreach with some work on victim assistance, but has not undertaken much action to address prevention and enforcement. In relation to the above corrective actions, we found that:

1. Agency-wide communication tools have been adequately updated to educate and assist taxpayers with information about identity theft.

---

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

2. After a significant delay (2 years), agency-wide standards on information needed to substantiate identity theft claims were issued.

3. There were still problems with the use of closing codes for cases involving identity theft. Because of problems implementing a universal code, the IRS has had to use a manual process.

4. The IRS has developed an Enterprise Identity Theft Strategy; however, it does not have sufficient plans to proactively identify identity theft and take appropriate enforcement action.

The IRS has taken action to resolve identification number discrepancies. It has revised its internal procedures and worked with the Social Security Administration (SSA) to reduce the time needed to resolve "scrambled" SSNs. When two tax returns are filed under the same SSN and the IRS cannot determine the true owner of the SSN, the "scrambled" SSN is sent to the SSA for verification. In the interim months (which previously took up to 2 years), the affected taxpayers would not be entitled to credits and/or refunds related to their SSN. The IRS is also updating its processes and notices to provide help to taxpayers whose names and SSNs have been used by an identity thief for employment purposes.

The IRS does not take any specific actions to ensure appropriate tax withholding for persons employed with a stolen identity—threshold amounts for the withholding compliance program are too great to have any impact on most employment-related identity theft cases.

Furthermore, although the IRS said it would work with employers through several initiatives to reduce the incidence of employment-related identity theft, there has been very little effort in this area and the IRS has indicated that it does not plan to do more to reduce this problem.

We plan to perform a follow-up audit on IRS identity theft actions in 2009. In addition, because some identity theft tax refund fraud makes use of direct deposit to commit the fraud, we have just completed an audit of IRS controls over direct deposits and will be issuing a report in September 2008.

c. What can the IRS do within 3 months, 6 months and a year to establish an IRS function that is fully responsible and accountable to ensure a corporate strategy that will find identity theft early and even stop it before it starts?

RESPONSE:

In response to a request by Chairman Baucus, the IRS stated that it would, within 3 months, provide a status report on its 5-year identity theft strategy—specifically, its goals, timelines, and milestones. The IRS provided an update on its Identity

Protection Strategy, but this document did not provide much additional clarity on its goals, timelines, and milestones. We believe that to better evaluate its progress, the IRS still needs more specific goals, timelines, and milestones. Furthermore, specific information is needed on the additional actions the IRS plans to take to pursue and prosecute individuals who are responsible for tax-related identity theft.

Within 6 months, the IRS indicated that the Identity Theft Assistance Unit would be trained, established, and functioning. We believe the Identity Theft Program Office should also conduct an analysis to ensure effective use of the new universal identity theft indicator so that taxpayers victimized by identity theft are not burdened by multiple IRS contacts for the same identity theft issue. Thereafter, the IRS should conduct such analysis annually.

Within a year, the IRS should be in a position to assess the successes and limitations of the corporate strategy so that it could make any revisions before formulating an annual plan for allocating resources and undertaking actions necessary for continued progress. The IRS assessment also should determine whether actions have facilitated and improved the coordinated responses of other agencies, such as the Social Security Administration and Federal Trade Commission.

d. What goals, milestones and timelines are appropriate to measure the IRS's progress toward developing an adequate identity theft strategy?

RESPONSE:

We believe the following goals would be appropriate:

- No multiple contacts to lawful taxpayers (in the same or consecutive years) by IRS for the same identity theft issue.
- A meaningful decrease over time of identity theft case counts.
- An increase in identity theft investigations and prosecutions.
- Implementation of preventive or detective measures.

We will be in a better position to assess the appropriate milestones and timelines when the IRS provides additional information on the resources it plans to devote to this effort.

2. In your written testimony, you state that some of the procedural changes made in 2006 to the Questionable Refund Program "may have adversely affected the IRS's ability to prevent potentially fraudulent refunds from being issued." How do you suggest that the IRS consider modifying the Questionable Refund Program in order to maintain a balance between taxpayer rights and tax administration, while still remaining strong enough to identify potential cases of identity theft?

RESPONSE:

One of the IRS changes in 2006 was to stop placing a Criminal Investigation (CI) freeze on the subsequent years' returns if the current return was determined to be fraudulent. The IRS made this change to address concerns raised by the Taxpayer Advocate regarding deficiencies with the Questionable Refund Program (QRP). However, the subsequent year freeze will protect the refund for an identity theft victim if the perpetrator tries to use the victim's SSN the following year to steal the refund. In our report,[2] we stated that when properly identified and worked in a timely manner, frozen refunds involving identity theft protect revenue and the innocent taxpayer. We recommended that the Chief, CI, consult with other IRS functions and reconsider placing a CI freeze on the subsequent years' returns of those accounts identified as fraudulent, including those returns involving identity theft. We continue to believe that the IRS should modify the QRP by freezing (or otherwise identifying) the subsequent account when the QRP determines a false refund was issued due to identity theft.

Any taxpayer who is the victim of identity theft will likely have contact with the IRS. The IRS's goal should be to promptly identify cases, quickly notify and correct the account of the affected taxpayer, and prevent the identity thieves from receiving inappropriate refunds. Some of the changes made by the IRS since 2006 to reduce the burden on taxpayers include issuing taxpayers a notice whenever it freezes a refund and releasing the refund within a certain number of days if it is not determined to be false. This process helps to maintain the taxpayers' rights. Further, freezing the subsequent year's account will help identify potential repeat instances of identity theft and prevent the issuance of additional false refunds. We believe these processes, along with our recommendation to reinstitute the subsequent year freeze, will maintain a balance between taxpayer rights and tax administration, while preserving the ability to identify potential cases of identity theft.

---

[2] *Actions Have Been Taken to Address Deficiencies in the Questionable Refund Program; However, Many Concerns Remain, With Millions of Dollars at Risk* (Reference Number 2007-10-076, dated May 31, 2007).

3. **Mr. George, your testimony states that you believe the IRS should use tax disclosure authorizations in the Internal Revenue Code to share certain tax related identity theft information with other Federal agencies to help deter and stop identity theft.**

    a. **Which agencies could the IRS share this information with?**

RESPONSE:

The Social Security Administration and Federal Trade Commission (FTC).

    b. **How would sharing this information help prevent tax related identity theft?**

RESPONSE:

Use of another person's identity for employment results in the misreporting of income, which affects income tax and social security tax as well as other employment taxes. Agencies with jurisdiction over these matters include the IRS and the SSA. Consequently, coordination between these agencies is important to ensure that Federal records related to income earned by a taxpayer are correct and to ensure appropriate law enforcement. Federal law[3] allows the SSA to pursue criminal penalties for an individual who fraudulently obtains, uses, or represents a SSN to be theirs.

The FTC is the agency responsible for tracking identity theft complaints. Once identity theft incidents are reported to the FTC, they are entered into the ID Theft Data Clearinghouse and are supposed to be shared with the law enforcement agencies that use the database to investigate and prosecute identity crimes. The IRS is not using the data for this purpose. We believe the IRS should use the FTC data for its intended purpose: to investigate and prosecute identity crimes. Moreover, it should provide data updates to the FTC and information that may otherwise be useful.

---

[3] 42 U.S.C. § 408 provides criminal penalties for the misuse of a social security card and/or account number.

4. **Mr. George, your office has performed many reviews of IRS security procedures. You have tested the security of IRS computer systems, how well IRS employees observe security procedures and the access of contractors to taxpayer data. Just recently, the State Department disclosed that contractors had made unauthorized access to the passport files of several presidential candidates.**

    a. **How well does the IRS protect taxpayer data? What are some of your most significant findings?**

RESPONSE:

TIGTA is responsible for detecting and investigating the unauthorized access of returns and return information. In fact, auditors from the State Department Inspector General's office recently visited with us to learn how we carry out this responsibility. TIGTA uses a computer-based detection program that analyzes access to tax accounts and identifies those with potential unauthorized access issues. Cases with confirmed issues are forwarded to TIGTA special agents in the field for further investigation. Employees found to have committed unauthorized access are subject to Federal prosecution, termination of employment, or other disciplinary action. During the 6-month period between October 2007 and March 2008, TIGTA identified and analyzed 245 leads of potential unauthorized access and referred 120 potential criminal cases to TIGTA special agents. During this period, TIGTA's unauthorized access program resulted in 12 criminal prosecutions and 86 administrative actions against IRS employees.

The IRS maintains highly sensitive financial information on over 130 million taxpayers that must be protected. While TIGTA's unauthorized access program is directed at identifying employees browsing individual taxpayer accounts, the risk exists that intruders from foreign states, organized crime, and other persons with malicious intent could steal vast amounts of taxpayer information by exploiting weak computer security controls. To maintain adequate security of sensitive taxpayer data, the IRS must implement controls at all levels of its computer environment to guard against external intruders, as well as malicious employees and contractors who have been given access to IRS systems to carry out their responsibilities.

Computer security has been designated a material weakness by the IRS for the last 10 years. Some of our most significant findings have included:

- Employees continued susceptibility to social-engineering attempts;
- Managers giving employees access to systems they did not need;
- Key security employees not following security procedures, which allowed the IRS network system to remain vulnerable to insider attacks;

- The IRS and its contractors not integrating security controls into modernized computer systems; and
- Audit log information was either not available or not being analyzed to identify unauthorized intrusions into the IRS computer network.

b. What more should the IRS be doing to ensure that confidential taxpayer information is protected?

RESPONSE:

The three most critical weaknesses we continue to find in our audits include:

1. Employees and contractors are being granted access to systems they do not need;
2. There is a lack of compliance with standard configurations for operating systems, databases, and other network components;
3. There is a lack of audit trail information to detect unauthorized security events.

Particular attention should be given to the lack of audit trail information to identify suspicious actions, who did them, where they were done, and how they were done. With today's threat environment, it is absolutely critical that the IRS can detect and investigate unauthorized intrusions and audit trail information. Additional funding will be needed to provide sufficient audit trail information and should be seriously considered to address this deficiency.

5. To what extent is phishing a threat to taxpayer privacy? What more can be done to stop these schemes from proliferating?

RESPONSE:

Phishing poses a potentially huge threat to taxpayer privacy. Millions of taxpayers entrust the IRS with their sensitive financial and personal information. TIGTA investigations have identified significant *phishing* attacks on IRS programs, such as e-file. Criminal fraud is being perpetrated utilizing legitimate taxpayer identity and tax return information.

Criminals can easily impersonate the IRS or any other Government agency or business on the Internet with very limited investment of time and capital. As technology evolves, the ability of criminals to spoof Web sites becomes increasingly easier to accomplish. The best way to stop this criminal activity is to alert the public when new scams are identified, aggressively remove *phishing* sites from the Internet as soon as possible after they are detected, and utilize law enforcement techniques, when available. I discuss law enforcement techniques last because arresting one of

these criminals is difficult, if not impossible, because much of the *phishing* activity is actually launched from outside of the United States.

To protect the IRS's reputation and to minimize the impact on tax administration and taxpayer privacy, TIGTA and IRS are working aggressively to thwart *phishing* scams and to shut down *phishing* Web sites that surface on the Internet.

6. To what extent would the regulation of return preparers, including more thorough vetting of ERO applicants, affect the identity theft problem?

RESPONSE:

We do not have information to indicate that a significant portion of the identity theft cases are related to return preparers or Electronic Refund Originators (ERO). However, there are other indications that regulation is needed. A recent review we performed indicates that the quality of return preparation among unenrolled preparers is a problem. Most tax returns prepared by a limited sample of unenrolled preparers contained significant errors, and some contained deliberate misstatements and omissions by the preparers. Our report on this will be issued in September 2008.

Electronic Return Originators are subject to tax compliance checks, validation of professional certification, confirmation of age requirements, and criminal background checks, which reduce the risk of integrity problems with *e-file* Providers.[4] However, in September 2007, TIGTA reported that the IRS only conducts limited criminal background checks and does not conduct credit checks.[5]

In response to another TIGTA report,[6] IRS management responded that credit checks were not performed because they were ineffective. *E-file* providers also raised concerns that their credit history reports showed inquiries by the IRS. IRS management previously indicated that additional criminal background checks are not necessary and cited an IRS business case study, which showed that, while 10 percent of the investigations revealed a criminal history, the information was usually not significant enough to deny participation in the *e-file* Program. IRS Management's position on not performing credit checks and limiting criminal background checks has not changed.

---

[4] An *E-file* Provider can be an Electronic Return Originator, Transmitter, or Software Developer.
[5] *Better Screening and Monitoring of E-File Providers Is Needed to Minimize the Risk of Unscrupulous Providers Participating in the E-File Program* (Reference Number 2007-40-176, dated September 19, 2007).
[6] *E-File Providers Are Not Adequately Screened* (Reference Number 2002-40-111, dated June 27, 2002).

Senator Grassley

1. **Most of the testimony this morning has focused on improving efforts to identify, track, and resolve cases of identity theft after they happen. While these efforts are critically important, it seems to me that with minimal effort, the IRS could help prevent identity theft before it happens.**

   As I noted in my opening statement, the IRS already uses a knowledge-based verification system to track refunds and permit electronic filing.

   If the IRS simply added a box to the printed tax forms – adjacent to the signature box – that allowed taxpayers to enter their previous year's AGI, it would go a long way toward preventing fraudulent tax returns.

   For those who lost last year's return, the IRS could simply hold their refund until April 15th to insure no one else files a return with the same name and social security number.

   Could you comment on this proposal?

   RESPONSE:

   Adding such a requirement would provide additional authentication, but would have certain limitations.

   - Some lawful taxpayers might not have last year's AGI or might not record the information correctly (i.e., rounding the AGI, transposition errors, etc.), which could cause their refund to be held or rejected.

   - In the instances that tax fraud related to identity theft is perpetrated by someone that the taxpayer knows (i.e., friend, relative, business associate, tax practitioner, etc.), this control might not prove to be effective, because they might have access to the taxpayer's prior year tax return information.

   - This proposal would not prevent employment-related identity theft—it would not stop the use of someone else's identity for employment. In many instances, a tax return is never filed for income earned using someone else's identity.

2. **In addition, as I noted in my opening statement, last year's immigration bill included a provision to allow workers to place a block on their Social Security number – much like the FTC do not call list, or a credit freeze.**

   To prevent fraudulent tax returns, taxpayers could place a block on their SSN until they file their own return. An identity thief who tried to file a return before the taxpayer did would not be able to collect a refund because the SSN would be blocked, thereby alerting the IRS to the fraudulent return.

   Could you comment on this proposal?

   RESPONSE:

   Such a block could help prevent fraudulent returns; however, an authentication mechanism would be needed first to allow the taxpayer to put the block on the account, then again to allow the lawful return through the system.

   As noted in our response to the previous proposal, in the instances that tax fraud related to identity theft is perpetrated by someone that the taxpayer knows (i.e., friend, relative, business associate, tax practitioner, etc.), this control might not prove to be effective, because they might have access to the information used to authenticate the taxpayer. Furthermore, *phishing* scammers might also attempt to obtain the taxpayer's method of authentication.

   This proposal would not prevent employment-related identity theft—it would not stop the use of someone else's identity for employment. In many instances, a tax return is never filed for income earned using someone else's identity.

Senator Snowe

1. **One method of online identity theft, phishing, seems to be spiraling out of control. More than 3.5 million Americans lost money to phishing schemes and online identity theft over a 12 month period ending in August 2007—this is a 57 percent increase over the previous year. And the total amount lost by the victims, $3.2 billion dollars.**

   Over the past 6 months the IRS has issued six separate warnings on phishing scams related to the IRS, and has significant information on suspicious emails and identity theft—including what steps taxpayers can take to protect themselves.

   While consumer awareness is critical in fighting against identity theft and phishing scams, can't there be more done legislatively to provide greater enforcement and stiffer penalties to act as a deterrent to curtail criminals from engaging in these fraud activities? If we just focus on awareness that might not reduce the prevalence of phishing scams, right?

   RESPONSE:

   While critical, we agree that a focus only on awareness will not necessarily reduce the prevalence of *phishing* scams and other forms of identity theft. Additional preventive measures, enforcement, and prosecution are needed to reduce this ever-changing crime problem. We have considered potential legislative changes that would assist in combating the proliferation of *phishing* scams. Unfortunately, the biggest obstacle to combating this crime is that much of it is launched from outside the U.S.

   Combating and thwarting identity theft requires a multi-faceted approach by which we leverage the resources of Federal and State law enforcement agencies, Internet Service Providers, and private companies. The IRS and TIGTA have coordinated efforts and combined their resources to address *phishing* scams and other forms of identity theft. Those efforts include:

   - Coordinating with the IRS Office of Online Fraud Detection and Prevention to identify and shut down fraudulent e-file *phishing* sites;
   - Working with Federal and State law enforcement agencies in conjunction with the Department of Justice's Computer Crime and Intellectual Property Section;
   - Coordinating with the U.S. Computer Emergency Readiness Team (CERT) at the Department of Homeland Security; and
   - Working with various Internet Service Providers and international CERTs to have the *phishing* sites taken offline as soon as they are reported.

2. **In 1998, Congress established a goal for the IRS that, by 2007, 80 percent of all returns be filed electronically. However, approximately 58 percent of individual taxpayers filed electronically last year. The IRS said it expects to reach the 80 percent milestone by 2012.**

   If phishing and other online tax scams continue to persist, will it hamper our ability to reach the goal we set 10 years ago?

   RESPONSE:

   These scams could have an effect. Taxpayers' perceptions of the security of their data affect whether they file electronically. The IRS must assure taxpayers that their electronic tax return information is secure. The IRS must continue to educate taxpayers on the importance of electronically accessing IRS information via the IRS's secure Web site (irs.gov). This will help to diminish the ability of individuals who employ *phishing* and other online tax scams to obtain information (names, SSN, and tax data) needed to file fraudulent tax returns. Furthermore, as the IRS moves toward communicating with taxpayers electronically, new methods need to be developed to ensure that taxpayers can verify the legitimacy of the communication.

   Notwithstanding the security concerns, there are other significant factors, such as the cost of e-filing and the concerns of taxpayers and preparers that if they file electronically, the IRS will have more data in its computers with which to perform compliance checks. As such, the IRS is likely to only meet the 80 percent goal if electronic filing is made mandatory for tax preparers and the cost of electronically filing decreases for taxpayers.

3. **In its Semiannual Report to Congress for April 1 – Sept 30, 2007, the Treasury Inspector General for Tax Administration stated that it considers major IRS programs to be highly at risk due to the increased frequency and complexity of electronic crimes in the United States. TIGTA was particularly concerned with Phishing. Furthermore, TIGTA stated that oversight of phishing of this area is necessary to ensure that misuse of the IRS name, impersonation of an IRS employee, and the identity theft incidents are resolved properly. In response to this report, the IRS agreed that more needs to be done with phishing and identity theft, including greater coordination with other agencies such as the Federal Trade Commission.**

   Could you elaborate on what greater coordination efforts could exists between the IRS and FTC to combat the problem of identity theft and phishing?

   RESPONSE:

   According to the FTC and the President's Identity Theft Task Force, once identity theft incidents are reported to the ID Theft Data Clearinghouse, the complaint will be

entered into the Clearinghouse and shared with law enforcement agencies that use the database to investigate and prosecute identity crimes. The fact that the IRS, by its own admission, is not using the data for this purpose directly contradicts information provided by the FTC and the President's Identity Theft Task Force.

We are concerned with the IRS's position that the FTC data is not useful in evaluating or investigating identity theft—especially given the rapid increase in tax-related ID theft. Because the Identity Theft Clearinghouse is the sole national repository of consumer identity theft complaints, it should be an important source of data for the Criminal Investigation Division.

In response to our report, the IRS did state that it is beginning to collaborate with the FTC in outreach activities and use general information from the ID Theft Clearinghouse to track trends, develop process improvements, and offer outreach initiatives for victim assistance. However, we believe the IRS should do much more than make use of general information from the Clearinghouse. It should use the specific data for its intended purpose: to investigate and prosecute identity crimes. It should also provide feedback to the FTC on data that is not correct or useful.

Senator Schumer

1. **Inspector George, in your written testimony, you point out that the IRS was quick to make changes suggested by the Taxpayer Advocate to protect taxpayer rights, but has not responded at all to several Inspector General reports highlighting inadequacies in the IRS's computer systems. How should the IRS balance its dual commitments to nondisclosure of taxpayer information and the need to alert employers and employees to possible cases of identity theft?**

   RESPONSE:

   Certain disclosure is permitted to help ensure that the information submitted by the employer is correct. The Social Security Administration (SSA) sends 'no-match' letters to employers when the name and SSN on the employee's W-2 does not match the SSA's records.

   A similar process is needed when both the name and SSN match SSA records, but there is evidence that neither belong to the employee submitting the information (such as confirmation by the lawful taxpayer that the earnings are not theirs). In such instances, the employer already has the name and SSN (which the employer assumes is legitimate) and the associated earnings. There should be no additional disclosure other than to notify the employer of the potential duplicate use of the identity, which necessitates further authentication.

Statement of Senator Charles E. Grassley
Senate Committee on Finance
Hearing on
Identity Theft: Who's Got Your Number?
April 10, 2008

Most Americans look forward to each year's tax filing season with mixed feelings of trepidation and anticipation. Will they owe more taxes or will they get a refund? But, for a growing number of taxpayers, tax filing season has become the source of another fear – that of becoming a victim of identity theft.

In recent years, the number of taxpayers who discover someone has used their name and Social Security number to illegally obtain a job or file a fraudulent tax return has increased dramatically, although the lack of comprehensive data makes it impossible to know the exact number.

But, there is no doubt identity theft is a growing problem. In my role as a member of the Judiciary Committee, I have supported efforts to increase penalties for those who commit this crime. However, as our witnesses today will explain, much more needs to be done to deter would be thieves and protect potential victims.

Despite ongoing efforts to modernize its computers, the IRS remains vulnerable to outside hackers and rogue employees who seek to improperly access taxpayer data. Preventing unauthorized access to IRS computers should be a top priority.

Another area that must be addressed is the illegal use of names and Social Security numbers by unauthorized workers. Congress attempted to address this issue last year in the immigration bill through an electronic employee verification system that allowed workers to block their SSN to prevent its illegal use. I have been working on similar legislation to allow every American to block their SSN and I hope to introduce it soon.

Finally, IRS should implement a knowledge based identity verification system to protect taxpayers from fraudulent tax returns. For example, taxpayers are allowed to check on the status of their income tax refund by using the dollar amount of their refund as their password.

Taxpayers may also use the self-select PIN option to file their return electronically by using their last year's AGI as their password. The IRS should implement similar procedures to protect every taxpayer from fraudulent returns.

Solving the problem of taxpayer-related identity theft will require a coordinated effort by both the IRS and the Congress. I look forward to working with the agency and my colleagues in the Senate to address this problem.

Written Statement of

Nina E. Olson

National Taxpayer Advocate

Before the

Committee on Finance

United States Senate

Hearing on

Identity Theft in Tax Administration

April 10, 2008

Chairman Baucus, Ranking Member Grassley, and distinguished Members of the Committee:

Thank you for inviting me to testify at today's hearing. In this written statement, I will first address the subject of identity theft in tax administration and then provide my perspective on two other significant tax administration issues – the need for legislation to improve tax administration, which this Committee has twice approved but has not been enacted into law, and the need for the IRS to take a more taxpayer-centric approach to e-filing issues.[1]

Because this hearing is taking place near the end of the 2008 filing season, I want to begin by commending the IRS for the admirable job it has done, particularly in light of the significant challenges it is facing. As I noted in my Annual Report, late-year tax-law changes impact both taxpayers and the IRS, and the uncertainty surrounding such changes increases the risk that problems will arise with basic service delivery and return processing.[2] These challenges increase when the IRS must devote substantial resources during the filing season to a major new initiative, such as preparing to pay out the recently authorized economic stimulus payments. To deliver these payments, the IRS not only must process payments to the over 130 million taxpayers who currently file income tax returns, but it also must identify and process returns from and payments to more than 20.5 million persons who have no filing requirement.[3] All of these exigencies divert the IRS from other important work, yet the fact that the IRS has managed to turn on a dime and deliver this filing season with no significant glitches is a testament to the extraordinary people who work at the IRS.

There are always tasks the IRS could perform better – and I will address some of them below – but I think it is important to take a moment to reflect on the vast responsibilities the IRS must meet to collect the revenue that our government requires to function and to acknowledge how much the IRS does very well.

---

[1] The views expressed herein are solely those of the National Taxpayer Advocate. The National Taxpayer Advocate is appointed by the Secretary of the Treasury and reports to the Commissioner of Internal Revenue. However, the National Taxpayer Advocate presents an independent taxpayer perspective that does not necessarily reflect the position of the IRS, the Treasury Department, or the Office of Management and Budget. Congressional testimony requested from the National Taxpayer Advocate is not submitted to the IRS, the Treasury Department, or the Office of Management and Budget for prior approval. However, we have provided courtesy copies of this statement to both the IRS and the Treasury Department in advance of this hearing.

[2] *See* National Taxpayer Advocate 2007 Annual Report to Congress 3-12 (Most Serious Problem: The Impact of Late-Year Tax-Law Changes on Taxpayers).

[3] Approximately 20.5 million persons received Social Security or Veterans' benefits and are therefore likely to qualify for stimulus payments but did not file tax returns in 2006. IRS News Release, *Special Economic Stimulus Payment Packages Go to Social Security, Veterans Recipients*, IRS-2008-37 (Mar. 10, 2008). There is also an unknown number of low income taxpayers who ordinarily would not have a filing requirement but will have to file this year to receive a payment.

I. Identity Theft in Tax Administration[4]

Identity theft is the number one consumer complaint in the United States, far outpacing all others.[5] Identity theft impacts tax administration when an individual intentionally uses the Social Security number (SSN) of another person to file a false tax return or fraudulently obtain employment. Misuse of another person's SSN or identity generally occurs in tax administration in two contexts: (1) the filing of a false return to obtain a fraudulent refund ("refund fraud") or (2) the theft and use of another person's SSN to obtain employment ("employment-related fraud").

In refund fraud, the perpetrator files early in the filing season using the personal information of the innocent taxpayer and before the lawful owner of the SSN has an opportunity to file. Typically, a perpetrator will use false Forms W-2 reflecting phantom wages and withholding credits, thus forming the basis of a fraudulent claim for a refund. To secure the fraudulent refund, the perpetrator typically will direct the IRS to transmit the refund electronically to a bank account under his or her control. When the identity theft victim later attempts to file his or her tax return, the IRS flags it as a "duplicate" return and freezes the refund.

In employment-related fraud, persons without the necessary legal status to obtain employment in the United States unlawfully use another person's SSN to appear work eligible. The employer of the undocumented worker will file a Form W-2 reflecting the worker's wages, which IRS data systems will attribute to the rightful SSN owner. The IRS will assess additional tax unless the lawful owner of the SSN acts to halt the erroneous assessment.

Regardless of the motive, identity theft results in serious consequences for the innocent taxpayer. Such consequences may include (1) the delay or denial of refunds, (2) the assessment of tax debts resulting from income reflected on the fraudulent filer's return, and (3) the requirement for victims to prove their identity to the IRS year after year. The IRS has a duty to these taxpayers to expeditiously determine the true owner of the SSN and to restore the integrity of the affected taxpayer's account.

---

[4] *See* National Taxpayer Advocate 2007 Annual Report to Congress 96-115 (Most Serious Problem: Identity Theft Procedures); *see also* National Taxpayer Advocate 2005 Annual Report to Congress 180-191; National Taxpayer Advocate 2004 Annual Report to Congress 133-136; National Taxpayer Advocate FY 2008 Objectives Report to Congress 15-16, 36-40; National Taxpayer Advocate FY 2006 Objectives Report to Congress iii-3; National Taxpayer Advocate FY 2005 Objectives Report to Congress 34.

[5] In 2007, the Federal Trade Commission (FTC) received 258,427 complaints of identity theft. The next closest complaint was shop-at-home catalog sales with 62,811 complaints. *See* FTC website, http://www.ftc.gov/opa/2008/02/fraud.pdf.

A. The IRS Is Unable to Quantify the Number of Identity Theft Incidents

I am concerned that the IRS does not know how many taxpayers are impacted by identity theft. Prior to January 1, 2008, the IRS had no method to systemically identify taxpayers whose identities were stolen. The IRS has now begun to track incidents of identity theft – but only in cases where the victim alerts the IRS *and* provides documentation verifying the identity theft and his or her identity. These conditions mean that many, and perhaps most, cases of identity theft will not be tracked by the IRS.

In employment-related fraud cases, for example, IRS data systems generally are able to detect a "name-SSN mismatch" (*i.e.*, cases where the taxpayer's name according to IRS data files does not match the associated SSN for that name). If an identity thief uses another taxpayer's SSN but the name does not correspond, the income on information returns (e.g., Forms W-2 or Forms 1099) bearing the SSN will not be attributed to the rightful SSN owner.[6] While this result spares the victim immediate headaches, it also means that an identity theft marker will not be applied, even though it is clear that the SSN has been misused. In addition, the rightful SSN owner will not receive notification that his or her SSN is being misused by another person. As discussed below, there are additional circumstances under which the identity theft marker will not be applied in cases of identity theft.

Thus, even with the electronic indicator of identity theft, it is apparent that the IRS will not be able to accurately quantify the number of identity theft cases. My personal belief is that the IRS has many more cases of identity theft on its hands than it is estimating. My employees report that they are now receiving calls from senior citizens who filed for the economic stimulus payment after not filing for years, only to find that someone else had been using their SSN on tax returns. To its credit, the IRS has recently established procedures that would allow its Taxpayer Assistance Centers (TACs) to process economic stimulus payments to identity theft victims who file solely to obtain the stimulus payment.[7] However, one wonders why the TACs cannot do this for similarly situated taxpayers in other tax return contexts.

B. Taxpayers Are Essentially Victimized Twice – Once by the Identity Thief and a Second Time by IRS Procedures that Prevent Them from Claiming Tax Benefits to Which They Are Entitled

In talking with my local taxpayer advocates and case advocates, I often hear that there is a lack of adequate procedures available to IRS employees to address the increasingly common crime of identity theft. In some respects, the IRS tries to fit a round peg into a square hole when addressing identity theft issues by using so-

---

[6] IRM 4.19.3.4.1 (Nov. 8, 2005).

[7] *See* IRS, SERP Alert, *Economic Stimulus Payment TAC Site Procedures for Identity Theft Situations* (Mar. 27, 2008).

called "mixed entity" procedures[8] and "scrambled SSN" procedures,[9] which were initially designed to address very different circumstances. As a result, there are significant gaps in the portion of the Internal Revenue Manual (IRM) that prescribes the IRS's procedures for handling identity theft cases.

A taxpayer contacting the IRS about his or her tax problem – usually involving a delayed refund or in response to an examination or collection notice for income that the taxpayer did not earn – generally does not know that he or she is the victim of identity theft. The IRS customer service representative, researching the delayed refund on IRS systems, will observe a duplicate return filing. The IRS will then send the first 239C letter, Scrambled SSN Clarification to Taxpayer, to each of the taxpayers using the SSN. This initial 239C letter informs the recipient that there may be a problem with the SSN used on his or her return, requests proof of the taxpayer's identity, and includes a questionnaire that inquires about the filer's past use of the SSN. Up to this point, the IRS has not told the taxpayer that another person is using his or her SSN, nor has an IRS representative attempted to contact the taxpayer by phone. Thus, the taxpayer has not yet been advised that he or she is a victim of identity theft.

Under current IRS guidance, if none of the SSN users respond to the first 239C letter within 40 days, the IRS institutes the "scrambled SSN" procedures. Similarly, if both of the taxpayers respond to the first 239C letter, the IRS institutes scrambled SSN procedures. In order to avoid scrambled SSN procedures, a taxpayer must timely submit documentation (1) validating the taxpayer's identity (such as a driver's license, passport or Social Security card)[10] and (2) verifying the existence of identity theft (*e.g.*, an affidavit of identity theft obtained from the Federal Trade Commission website or a copy of a police report).[11]

When the IRS institutes its scrambled SSN procedures, it assigns a temporary tax identification number, called an IRS number or "IRSN," to each user of the SSN, including the victim of identity theft.[12] A second 239C letter instructs each user of

---

[8] The IRS uses "mixed entity" procedures when it knows which of the multiple SSN users the rightful owner is. Under mixed entity procedures, the IRS assigns a temporary IRS number (IRSN) to taxpayer(s) wrongfully using the SSN, while the rightful SSN owner can continue using the SSN. The IRS then separates out the income attributable to the fraudulent filer from the innocent taxpayer's account, transferring the disputed income to the IRSN. *See* IRM 21.6.2.4.3 (Oct. 1, 2007).

[9] The IRS uses "scrambled SSN" procedures when it cannot determine the true owner of the SSN. In this situation, it assigns IRSNs to both (or all, if more than two) taxpayers who used the common SSN. The IRS instructs taxpayers who are assigned IRSNs to discontinue using their SSN. *See* IRM 21.6.2.4.4 (Oct. 1, 2007).

[10] *See* IRM 21.6.2.4.4 (Oct. 1, 2007).

[11] *See* Memorandum on Standard Identity Theft Documentation, Deputy Commissioner for Services and Enforcement, Kevin M. Brown (June 11, 2007).

[12] In FY 2005, the IRS assigned IRSNs to over 77,000 taxpayers. However, identity theft victims are not the sole recipients of IRSNs. For example, in mixed entity cases, perpetrators of identity theft are assigned IRSNs. *See* IRM 21.6.2.4.3.1 (Oct. 1, 2007).

the SSN, including the identity theft victim, to use the IRSN to file his tax returns while the IRS and the Social Security Administration (SSA) seek to determine the rightful owner of the SSN in question, a process that has historically taken up to two years.[13] The second letter advises the taxpayer as follows:

> You should use the Internal Revenue Service Number (IRSN) for federal income tax purposes until we can verify your social security number (SSN). Your IRSN is only a temporary number.
>
> We cannot allow you credits such as the Earned Income Tax Credit, etc., unless you have a valid taxpayer identification number. However, you should file your return on time and claim any credits you are legally entitled to even though you cannot receive them until we verify your SSN.[14]

This letter is extremely confusing to taxpayers. First, the IRS tells the taxpayer that he must use an IRSN. Second, the IRS tells the taxpayer that because he is using an IRSN, he will not receive the EITC, or the child tax credit, or other such benefits. Finally, the IRS tells the taxpayer that he should claim those credits anyway, using the IRSN on the return. Given the confusing instructions of this 239C letter, the taxpayer might not claim the EITC or other tax benefits on his return out of fear of being audited.

At the same time, the taxpayer may begin to suspect that he is a victim of identity theft and would then have to begin the laborious process of placing a fraud alert on his credit records, working with creditors to determine the extent of any fraud that may have been committed in his name, taking steps to protect against further fraud, and working to clear his record. However, because the IRS has not clearly alerted the taxpayer of potential identity theft and its related consequences, it is also possible that the taxpayer might not take these necessary steps to protect himself. From the point of view of the affected taxpayer, the IRS instructions are very confusing.

Meanwhile, the IRS has not called the taxpayer to discuss any of these developments. All communication is done by correspondence, which might be sent to someone who has low literacy. Such an approach to likely victims of identity theft is hardly reflective of world class customer service. In fact, IRS procedures increase the harm to the victim by prematurely placing taxpayers into scrambled

---

[13] The IRS states that the average scrambled SSN case currently takes approximately ten months to resolve. This is a substantial reduction from prior periods and is attributable to recently implemented process improvements made by the IRS in collaboration with the Social Security Administration. *See* National Taxpayer Advocate 2007 Annual Report to Congress 110. However, the IRS cannot measure the actual cycle time of identity theft cases because the IRS has not tracked the incidence of identity theft in its cases, nor is it able to identify identity theft cases to enable it to pull a representative sample.

[14] IRM 21.6.2.4.4 (Oct. 1, 2007).

SSN procedures and by failing to utilize information already available to the IRS to avoid scrambled procedures.

In many instances, the IRS could avoid using scrambled SSN procedures by sending an initial notification and providing a phone number to a dedicated unit that could answer the taxpayer's questions and explain what is required for proof. In other instances, it is fairly easy to ascertain the correct owner of the SSN. For example, in several Taxpayer Advocate Service cases, including one I worked on, the owner of the SSN was a very young child. The IRS has access to various government databases that enable it to determine the age of the SSN owner, and in many cases we will know who is the mother, and sometimes the father, of the SSN owner.

If the SSN of a very young child shows up on a Form W-2 reporting wages from a full-time job, it should be fairly clear that that child did not earn those wages and should be treated as the victim rather than the perpetrator. We can at least avoid using scrambled SSN procedures with respect to these cases. Under current IRS guidance, however, such an account might be placed in scrambled SSN procedures, and the child's parents, in addition to having to straighten out the serious problem of identity theft, would be unable to claim the dependency exemption, child tax credit, and earned income tax credit (EITC) with respect to the child until the IRS and SSA reach a formal decision about the true holder of the SSN.[15]

This harm is compounded under the provisions of the recently enacted Economic Stimulus Act of 2008.[16] The Act provides that any return that does not include an SSN – whether for a primary or secondary taxpayer or a dependent – will be ineligible for the economic stimulus payment.[17] Thus, taxpayers who already are victims of identity theft are further victimized by IRS processes. These taxpayers in fact have an SSN. It is simply the IRS's and SSA's cumbersome processes that are causing these taxpayers to wait for and possibly lose up to two years' worth of dependency exemptions, child tax credits, and earned income tax credits – and now economic stimulus payments as well.[18]

---

[15] Treas. Reg. § 301.6109-1(a)(1)(i) provides that taxpayer identifying numbers (TINs) include SSNs, individual taxpayer identification numbers, adoption taxpayer identification numbers, and employer identification numbers. IRC § 151(e) requires any dependent to have a valid TIN; IRC §§ 32(c)(1)(E), (c)(3)(D), and (m) require the eligible taxpayer and the qualifying child to have valid SSNs.

[16] Pub. L. No. 110-185, 122 Stat. 613 (2008).

[17] *Id.*

[18] The economic harm inflicted by scrambled SSN procedures is considerable for low income taxpayers. Among taxpayers who received EITC benefits and received tax refunds in tax year 2005, the average refund amount was $3,093.46, and the average adjusted gross income was $15,484.52. *See* IRS Compliance Data Warehouse, Individual Returns Transaction File (Tax Year 2005). Thus, the average refund amounted to 20 percent of each taxpayer's annual income.

I have proposed that the IRS search its records to identify identity theft victims who were required by the IRS to use IRSNs on their returns, contact these taxpayers, and assist them in obtaining verification of their identities and proof of identity theft, so they will be able to receive the tax benefits to which they are entitled. If these taxpayers are to receive their economic stimulus payments this year, however, the IRS must act quickly. At the very least, it can instruct these taxpayers to claim the payment on their 2008 income tax returns.[19]

C. The IRS Is Taking Some Steps to Address Recurring Identity Theft

Identity theft is a recurring issue for many taxpayers; victims of identity theft often find themselves needing to resolve account problems with the IRS over multiple years. The IRS finally acknowledged this reality and recently implemented a tracking system through which an indicator will be placed on an identity theft victim's account once he or she has provided verification of identity theft. In subsequent filing years, the IRS will be alerted to the fact that a taxpayer with this identity theft indicator on his or her account may have special needs and require special handling and attention.

I am very pleased with this positive development, as my office has long advocated such a tracking system.[20] However, there are shortcomings to this tracking system. As illustrated above, the identity theft indicator will not capture certain types of identity theft. In addition, the IRS still does not track cases where the taxpayer does not respond or provides insufficient documentation of identity theft.[21]

Moreover, the IRS needs to take a much more taxpayer-centric approach to identity theft with respect to the identity theft indicator. For example, the IRS has no central guidance about how to apply the indicator, allowing each operating division and function to create its own procedures. Thus, an identity theft victim's account may be handled differently depending on which part of the IRS he or she contacts.

---

[19] The Taxpayer Advocate Service asked IRS Accounts Management personnel the rationale for using IRSNs in scrambled SSN situations, given that the practice results in the denial of the personal exemption. Accounts Management responded that IRSNs are used to separate tax data on scrambled cases until the owner of the common number is identified, and that the personal exemption must be denied until the Social Security Administration can determine who the true owner of the SSN is. Accounts Management further stated, "Consider that the same taxpayer may have filed all of the returns posted under the common number. Until sufficient information is received to resolve the case, the taxpayer should not be given the benefit of claiming the exemption again." Email from Accounts Management to TAS (Jan. 17, 2007). TAS has been unsuccessful in its attempts to persuade the IRS to modify its procedures.

[20] *See* National Taxpayer Advocate 2005 Annual Report to Congress 191.

[21] To its credit, the IRS is applying the TC 971 indicator on phishing cases without requiring the victims to provide the two types of documentation normally required.

D. The IRS Should Consider Centralizing Its Procedures to Assist Identity Theft Victims

Another concern is that there is no coordinated effort to address an identity theft victim's issues from start to finish. The IRS's Automated Underreporter, Automated Collection System, Criminal Investigation, Examination, and Accounts Management functions all work identity theft cases, but none of them is responsible for addressing all federal tax issues to make the taxpayer whole.[22] As a result, identity theft-related cases in the Taxpayer Advocate Service have increased substantially. In particular, TAS's stolen identity cases have increased by 644 percent from FY 2004 to FY 2007.[23]

In my 2007 report to Congress, I recommended that the IRS develop a dedicated, centralized unit to handle all identity theft cases and a centralized chapter in the IRM to house all identity theft procedures.[24] A centralized unit will be able to identify trends and systemic problems, and can serve as a central contact point for discussions with SSA to improve processing. With a centralized unit dedicated to resolving identity theft issues, victims of identity theft would have a single point of entry into the IRS and could more readily check on the status of their identity theft-related account issues. I am personally seeking agreement from the IRS leadership to work with me and my staff to develop such a unit and IRM.

---

[22] In fact, the IRS estimated that there are 17 entry points at which an identity theft case can come into the system. *See* IRS, *Identity Theft Program Current State* (July 20, 2007).

[23] The Taxpayer Advocate Service utilizes three primary issue codes to track identity theft cases. The table below shows the increase in Stolen Identity (primary issue code 425), Mixed Entity (primary issue code 410), and Scrambled SSN (primary issue code 420) cases from FY 2004 to FY 2007. The total number of identity theft-related cases may be underestimated due to the system's limitation of two issue code fields.

	FY 2004	FY 2005	FY 2006	FY 2007
Stolen Identity	447	922	2,486	3,327
Mixed Entity	1,681	1,493	2,062	2,303
Scrambled SSN	786	1,063	1,107	858
Total:	2,914	3,478	5,655	6,488

Taxpayer Advocate Management Information System (TAMIS), FY 2004, FY 2005, FY 2006 and FY 2007. TAS began tracking Stolen Identity cases in March 2004; the annual total for 2004 is a 12-month estimate based on an actual nine-month count of 335 cases.

[24] *See* National Taxpayer Advocate 2007 Annual Report to Congress 115.

E. The IRS Should Quickly Consider and Act on Recommendations Contained in the National Taxpayer Advocate's 2007 Annual Report to Congress

The Taxpayer Advocate Service has struggled for years with the problem of identity theft in its casework and reported on it in past Annual Reports to Congress.[25] In my most recent Annual Report to Congress, I identified IRS Identity Theft Procedures as the sixth most serious problem facing taxpayers.[26] The report included several significant recommendations to the IRS that would improve processes, minimize harm to the taxpayer, and improve its taxpayer service in this area. The specific recommendations, some of which are discussed in greater detail above, were sent to the Commissioner on February 29, 2008. Under IRC § 7803(c)(3), the IRS has three months to provide a formal response to these recommendations. The recommendations are as follows:

- The IRS should develop a dedicated, centralized unit to handle all identity theft cases, as well as a centralized IRM to house all identity theft procedures across the IRS. Such a centralized unit would be able to provide and monitor training to its employees and track cycle time and other quality measures. A centralized IRM would provide various alternatives for account resolution.

- The IRS should develop a form that taxpayers can file when they believe they have been victims of identity theft. The instructions on the form should explain which steps the IRS will take and which steps the taxpayer should take to restore the integrity of the taxpayer's account (*e.g.*, obtaining an FTC affidavit).

- The IRS should issue a notice to taxpayers whose refunds have been frozen because of a duplicate filing. A refund freeze can have the same effect as a refund denial if the taxpayer is unaware of the freeze or the reasons behind it.

- The IRS should also freeze collection actions when a duplicate filing is present until an investigation can determine whether an identity theft has taken place. Under current procedures, a duplicate return filing is not a sufficient basis to freeze the collection action.

- The IRS should eliminate Form 8453-OL, *U.S. Individual Income Tax Declaration for an IRS e-file Online Return,* from the electronic return process and make the use of personal identification numbers (PINs) mandatory. This

---

[25] *See* National Taxpayer Advocate 2007 Annual Report to Congress 96-115; National Taxpayer Advocate 2005 Annual Report to Congress 180-191; National Taxpayer Advocate 2004 Annual Report to Congress 133-136; *see also* National Taxpayer Advocate FY 2008 Objectives Report to Congress 15-16, 36-40; National Taxpayer Advocate FY 2006 Objectives Report to Congress iii-3; National Taxpayer Advocate FY 2005 Objectives Report to Congress 34.

[26] *See* National Taxpayer Advocate 2007 Annual Report to Congress 96-115.

step would increase security, save money, and help to eliminate taxpayer burden. Under current procedures, electronic filers who do not elect to use PINs in order to electronically file their returns must sign Form 8453-OL and mail it to the IRS. The IRS generally receives these forms after it has processed the e-filed return.

- The IRS should give identity theft victims the ability to take proactive measures such as blocking the e-filing option on their accounts.

- The IRS should plan an Identity Theft Summit to bring together all IRS functions that deal with identity theft issues to discuss the problems in a collaborative and comprehensive manner.

F. Preparers Should Be Required to Mask Social Security Numbers Before Transmitting Tax Return Information Abroad

Internal Revenue Code sections 7216 and 6713 impose criminal and civil sanctions, respectively, on preparers who, with the requisite level of intent, use or disclose tax return information, except where expressly permitted to do so by an exception provided in the statute or regulations. Pursuant to recently revised final regulations under Internal Revenue Code § 7216, preparers located in the United States will be prohibited from obtaining a taxpayer's written consent to disclose the taxpayer's Social Security Number to a return preparer located overseas as of January 1, 2009. Thus, preparers will have to redact or otherwise mask taxpayers' SSNs before disclosing tax return information outside the United States.[27] This provision originated from a recommendation made by the Taxpayer Advocacy Panel in order to protect taxpayers from identity theft.[28]

I am extremely pleased that the Treasury Department has adopted this taxpayer-friendly provision and shown leadership in combating the problem of identity theft. For an identity thief, another person's SSN is the most valuable tool he can obtain to commit financial fraud, and the SSN becomes even more valuable if it is linked to other personal data of the SSN owner, like information required to prepare a tax return. As we have discussed above, it is very difficult for a taxpayer to put the "genie back in the bottle" once his or her identity has been stolen. The difficulty is compounded if the theft occurs overseas, where the laws of the United States do not reach. Thus, it is incumbent on tax administration to take all necessary steps to protect taxpayers' SSNs from exposure.

The structure of IRC § 7216 reflects the urgency felt by Congress to protect the taxpayer identity and tax return information. The code section starts with a broad prohibition against the preparer's using or disclosing information provided for or in

---

[27] 2008-5 I.R.B. 344 (Feb. 4, 2008). The new requirement is effective January 1, 2009 and is set forth in Treas. Reg. § 301.7216-3(b)(4), as amended.

[28] Letter from Larry T. Combs, Chair, Taxpayer Advocacy Panel to Commissioner Mark W. Everson, (Aug. 18, 2006).

connection with preparing a return. The statute then provides three specific exceptions and authorizes the Secretary to prescribe regulations permitting other exceptions.

This statutory design mirrors that of another bedrock tax statute, IRC § 6103, which governs the disclosure of tax return information by the Internal Revenue Service. As with IRC § 7216, section 6103 starts with a sweeping prohibition against the IRS's disclosing any return or return information and requires any exceptions to be specified in the Internal Revenue Code itself. The approach common to both these statutes is no accident – confidentiality of a taxpayer's return information is absolutely necessary to maintain taxpayer confidence in the tax system and to the smooth operation of the system.

I find the approach adopted by Treasury in the final regulations to be remarkably balanced. In general, taxpayers may continue to consent to the disclosure of their tax return information overseas.[29] The regulation merely requires preparers to "mask" in some way the SSN of taxpayers when taxpayer information is sent overseas. In striking this balance, Treasury took note of the increased risk of harm when taxpayer data is sent abroad, where the means for oversight and remedies for harm are not as available as in the United States.

These concerns were first brought to light by the Taxpayer Advocacy Panel (TAP), a congressionally chartered Federal Advisory Committee created to advise the Secretary of the Treasury, the Commissioner of Internal Revenue, and the National Taxpayer Advocate to improve taxpayer service for individual and small business taxpayers.[30] The TAP is composed of volunteers from all walks of life, and brings a much-needed taxpayer perspective to tax administration. In a letter written in response to the IRS Commissioner's specific request for the TAP's comments, the TAP wrote:

> Outsourcing also increases the potential for identity theft and gross abuse of taxpayer data without adequate safeguards.... In addition to obtaining taxpayer consent, the preparer must be required to ... [e]nsure that when client data is sent to an offshore

---

[29] Taxpayers may knowingly consent to the disclosure of their tax return information to an overseas preparer for a variety of valid reasons, including to obtain expertise in international tax matters, to coordinate the filing of U.S. and foreign tax returns, or to receive the benefit of lower return preparation costs in some cases.

[30] *See* Federal Advisory Committee Act, Pub. L. No. 92-463 (5 U.S.C. App.); *see also* Charter for the IRS Taxpayer Advocacy Panel, available at http://fido.gov/facadatabase/docs_charters/5217_Charter_(2008-03-17-08-28-02).doc. The Taxpayer Advocacy Panel consists of approximately 100 members, with representatives from each state, the District of Columbia, and Puerto Rico. The Taxpayer Advocate Service provides funding and staffing to support the TAP. Annual reports are submitted to the Secretary of the Treasury and the Commissioner of Internal Revenue. Copies of all reports, event notices, meeting agenda and minutes, and success stories can be found on the TAP website at www.improveirs.org.

> location, personal data, such as Social Security Numbers (SSNs), date of birth, telephone number(s), and bank account information, is replaced with a combination client number or similar cross-identifier and the identifying information redacted, thus eliminating the dissemination of personal data outside the preparer's office.[31]

Practitioners have recently raised some legitimate administrability concerns about the redaction requirements in the new regulations, particularly with respect to the business practices of practitioners who provide tax preparation services to expatriates and other offshore taxpayers. However, I believe that these concerns can be addressed through an IRS notice or revenue procedure supplementing the regulation. None of these concerns is insurmountable, and some appear to me to be the result of an overly broad and restrictive reading of the regulation.

As sensitive as I am to practitioners' concerns, I firmly believe the SSN redaction requirement should remain intact. A taxpayer-centric approach to identity theft – such as the one the TAP urged and Treasury adopted – would protect the overwhelming majority of taxpayers while developing procedures to address the special needs of the few. The taxpayers in most need of SSN masking protection are less sophisticated taxpayers who contract with a domestic preparer, who do not expect their SSNs to be sent abroad, and who may not fully appreciate the consequences of transmitting one's data abroad. I believe a solution exists that will address preparers' concerns yet keep this important provision intact in the regulations to safeguard the majority of taxpayers from international identity theft.

Accordingly, I am not opposed to carving out narrowly targeted exceptions to the general prohibition against disclosing SSNs overseas in situations where a strong business case can be made that the benefits of allowing disclosure outweigh the increased risks of identity theft.[32] Further, if technology is at issue, it is always possible to extend the effective date of the relevant regulation sections to address these concerns. However, I believe it would be a serious mistake to tinker with the structure of the regulation, which mirrors the Internal Revenue Code's broad protection of taxpayer data, when there are ways to address these implementation issues through supplemental guidance.

---

[31] Letter from Larry T. Combs, Chair, Taxpayer Advocacy Panel, to Mark W. Everson, Commissioner, Internal Revenue Service (Aug. 18, 2006) (on file with the Taxpayer Advocate Service).

[32] This "balancing" test is consistent with Treasury's longstanding approach to exceptions under IRC § 6103. *See* Department of the Treasury, *Report to the Congress on Scope and the Use of Taxpayer Confidentiality and Disclosure Provisions. Vol. I: Study of General Provisions* (Oct. 2000); Staff of the Joint Committee on Taxation, *Study of Present Law Taxpayer Confidentiality and Disclosure Provisions as Required by Section 3802 of the Internal Revenue Service Restructuring and Reform Act of 1998. Vol. I: Study of General Disclosure Provisions*, JCS-1-00 (Jan. 28, 2000); National Taxpayer Advocate 2003 Annual Report to Congress 232-255.

II. Other Significant Tax Administration Issues

A. The Time Is Ripe for a Taxpayer Bill of Rights and for Related Legislation to Improve Tax Procedure[33]

On July 22 of this year, we will mark the tenth anniversary of the Internal Revenue Service Restructuring and Reform Act of 1998 (RRA 98), a landmark piece of legislation that established many significant protections for taxpayers in their dealings with the IRS. Over the last ten years, there have been many changes in the tax world – including a new batch of tax shelters, increasing identity theft, a greater ability to electronically track financial transactions, a large increase in the number of returns filed electronically, and an increased emphasis on tax law enforcement. Despite all of these changes, there has been no significant legislation in the taxpayer rights or tax procedure arena over the last ten years.

In my 2007 Annual Report to Congress, I recommend that Congress clarify taxpayer rights by creating a true "Taxpayer Bill of Rights" (TBOR). Modeled after the U.S. Constitution's Bill of Rights, this TBOR would serve as a clear statement of the social contract between the government and its taxpayers – that taxpayers agree to report and pay the taxes they owe and the government agrees to provide the service and oversight necessary to ensure that taxpayers can and will file and pay their taxes. I believe it is in the best interest of taxpayers and tax administration for this unspoken agreement to be explicitly articulated in a formal Taxpayer Bill of Rights, which should incorporate a clear statement of taxpayer rights as well as a statement of taxpayer obligations.[34]

I am hopeful a Taxpayer Bill of Rights may also serve as a vehicle for more comprehensive taxpayer rights and tax procedure legislation that fills some of the gaps identified since the passage of RRA 98. In recent years, the tax-writing committees have made efforts to pass such legislation. In 2003, the Ways and Means Committee reported and the full House approved the Taxpayer Protection and IRS Accountability Act,[35] and in 2004, the Finance Committee and the full Senate approved the Tax Administration Good Government Act.[36] However, no conference committee was formed, and the bills were never enacted. In 2006, the Senate Finance Committee tried again, approving a significant taxpayer rights and tax administration package as part of the Telephone Excise Tax Repeal Act, but it was not considered by the full Senate.[37]

---

[33] *See* National Taxpayer Advocate 2007 Annual Report to Congress 478-489 (Legislative Recommendation: Taxpayer Bill of Rights and *De Minimis* "Apology" Payments).

[34] For a discussion of the specific taxpayer rights and obligations, see National Taxpayer Advocate 2007 Annual Report to Congress 478-489.

[35] H.R. 1528, 108th Cong. (2003).

[36] S. 882, 108th Cong. (2004).

[37] S. 1321, 109th Cong. (2006).

The passage of time has only increased the need for such legislation. Among the proposals I believe should be included are the following:

- Protect the more than 60 percent of taxpayers who rely on paid tax preparers by imposing minimum standards of competence. At present, anyone can prepare federal tax returns; there are no standards at all. Preparers should be required to pass a basic competency test and take periodic Continuing Professional Education courses. Greater accuracy in return preparation will benefit both taxpayers and the IRS.

- Increase electronic filing by allowing taxpayers to prepare and file their returns electronically without having to pay a fee to private vendors. The IRS should make an e-filing template available and develop a direct filing portal. A direct filing portal will not only attract taxpayers concerned about costs but will also reassure taxpayers who have data security concerns about routing their personal tax information through third-party vendors.

- Protect low income taxpayers by regulating refund anticipation loans (RALs), especially by prohibiting cross-collection agreements.

- Reduce the burdens on partners in partnerships by advancing the initial partnership return filing deadline from April 15 to March 15. At present, partnerships generally cannot prepare Schedules K-1 on which they report each partner's income and other tax attributes until they finish preparing the full partnership return, and hundreds of thousands of partners receive their K-1s on or after April 15, requiring them to file for extensions.

- Protect low income senior citizens by exempting Social Security payments from levies or by requiring the IRS to develop and utilize an effective screen so that levies are not automatically imposed on taxpayers who are likely to suffer economic hardship.

- Simplify the "kiddie tax" computation rules.

This is not a comprehensive list of proposals that I believe should be adopted, but it represents a good start in combination with proposals included in prior legislation approved by the Finance Committee. I urge this Committee to take up the Taxpayer Bill of Rights this year.

B. The IRS Should Exert a Stronger Oversight Role in the Electronic Filing Arena[38]

While the IRS has made impressive progress in increasing the rate of electronic filing, it is still far from reaching the congressionally mandated goal of 80 percent.[39] During the 2007 filing season, almost 57 percent of all individual returns were filed electronically.[40] As the tax administrator, the IRS has the authority to determine the policies and criteria that entities must meet to participate in the e-file program. In important respects, however, it appears that the IRS has historically relinquished control of the electronic filing program to private industry and faces difficulty in re-asserting ownership of the program. Considering the significant benefits e-filing affords to both the IRS and taxpayers, we are pleased that the IRS is currently evaluating its role in the e-file program in order to increase the rate of e-file and to properly align its policies and procedures to meet the best interests of taxpayers and the agency itself. We encourage the IRS to consult with the National Taxpayer Advocate on this important matter, and we look forward to lending support in any manner possible.

1. To Fully Realize the Benefits of e-File, the IRS Should Enable All Taxpayers to Prepare Their Returns and File Directly with the IRS without Charge

The IRS has an incentive to increase the rate of electronic filing to the highest level possible. Electronic filing of tax returns brings benefits to both taxpayers and the IRS.[41] From a taxpayer perspective, e-filing improves accuracy by eliminating the risk of IRS transcription errors, pre-screens returns to ensure that certain common errors are fixed before returns are accepted, and speeds the delivery of refunds. From an IRS perspective, e-filing eliminates the need for data transcribers to input

---

[38] *See* National Taxpayer Advocate 2004 Annual Report to Congress 89-109 (Most Serious Problem: Electronic Return Preparation and Filing) and 471-477 (Legislative Recommendation: Free Electronic Filing for All Taxpayers); *see also* National Taxpayer Advocate 2007 Annual Report to Congress 83-95 (Most Serious Problem: The Use and Disclosure of Tax Return Information by Preparers to Facilitate the Marketing of Refund Anticipation Loans and Other Products with High Abuse Potential) and 547-548 (Legislative Recommendation: Authorize Treasury to Issue Guidance Specific to Internal Revenue Code Section 6713 Regarding the Use and Disclosure of Tax Return Information by Preparers); National Taxpayer Advocate 2006 Annual Report to Congress 197-221 (Most Serious Problem: Oversight of Unenrolled Preparers); and National Taxpayer Advocate 2005 Annual Report to Congress 162-179 (Most Serious Problem: Refund Anticipation Loans: Oversight of the Industry, Cross-Collection Techniques, and Payment Alternatives).

[39] The IRS Restructuring and Reform Act of 1998 directed the IRS to set a goal of having 80 percent of all returns filed electronically by 2007. *See* Internal Revenue Service Restructuring and Reform Act, Pub. L. No. 105-206, § 2001(a)(2), 112 Stat. 685 (1998). The 80 percent e-filing goal was not achieved by 2007. However, we believe Congress should reiterate its commitment to requiring the IRS increase the e-filing rate as quickly as possible.

[40] IRS News Release, *IRS E-File Opens for 2008 Filing Season for Most Taxpayers,* IR-2008-5 (Jan. 10, 2008).

[41] *See* S. Rep. No. 105-174, at 39-40 (1998).

return data manually (which permits the IRS to shift resources to other areas), allows the IRS to capture return data electronically, and enables the IRS to process and review returns more quickly.[42]

Nearly one-third of all individual returns processed by the IRS through October 2007 – or 43 million returns – were prepared using software yet mailed in rather than submitted electronically.[43] These taxpayers could have e-filed their returns once they were prepared using computer software, but for some reason, the taxpayers chose to file paper returns. If the IRS successfully converts a significant portion of these taxpayers to electronic filing, it would approach, and perhaps surpass, the 80 percent e-filing goal.

I have advocated for years for the IRS to place a basic, fill-in template on its website to permit taxpayers to self-prepare their tax returns and file directly with the IRS for free.[44] There is no reason why taxpayers should be required to pay transaction fees to file their returns electronically. A free template and direct filing portal would address some taxpayers' cost and security concerns and would result in a greater number of e-filed tax returns. For those taxpayers who are comfortable preparing their returns without assistance, the government should provide the means for them to do so without charge. For those taxpayers who do not find a basic template sufficient and would prefer to avail themselves of the additional benefits of a sophisticated software program, they will remain free to purchase one.

During a visit to the Australian Taxation Office (ATO) last month, I had the opportunity to learn first-hand about Australia's e-file program. The ATO built e-tax, a direct filing program, completely in-house and officially launched the program in 1999. The resulting e-file (e-tax) rates are impressive.[45] For the 2005-2006 tax year, approximately 49 percent of all individuals who self-prepared lodged their returns through e-tax, compared to approximately 8 percent of U.S. taxpayers who self-prepared their returns using Free File for tax year 2006.[46] Further, only tax

---

[42] *See* IRS Fact Sheet, *2008 IRS E-File,* FS-2008-4 (Jan. 2008).

[43] IRS Tax Year 2006 Taxpayer Usage Study (through Oct. 26, 2007).

[44] *See, e.g.,* National Taxpayer Advocate 2004 Annual Report to Congress 471-477. We have proposed that the IRS create an electronic tax return that is analogous to the paper environment, but that also incorporates the benefits of electronic technology. Specifically, the return should be fill-in, with math checking and number-transfer capability. The fill-in return should link to line-by-line IRS instructions for each form, and where the IRS instructions reference a publication, there should be active links to specific sections of the forms. Where the instructions or publications have worksheets embedded in them, these worksheets should be fill-in, with math-checking and number-transfer capability. These capabilities are important, since they will substantially reduce the number of "math error" notices the IRS must issue each year.

[45] Unlike Free File, e-tax is available to taxpayers at all income levels. For information on e-tax, see http://www.ato.gov.au/corporate/content.asp?doc=/content/83847.htm&pc=001/001/001/005&mnu=&mfp=&st=&cy=1 (last visited April 7, 2008).

[46] Australian Taxation Office, Taxation Statistics 2005-06, available at http://www.ato.gov.au/content/downloads/00117625_2006CH2PER.pdf (last visited April 7, 2008); E-

agents (the Australian equivalent to tax return preparers) use commercial software to prepare and file returns.[47] It is our understanding that the IRS is currently evaluating the Australian taxation system. We hope the IRS can apply lessons learned from Australia's experience to our own e-file program, especially with regard to ATO's direct filing program, e-tax.

Recent, highly publicized phishing schemes confirm the need for the IRS to develop a free fill-in template and direct filing portal. During the 2007 filing season, for example, an Internet tax scam lured taxpayers into entering confidential tax return information on sites masquerading as Free File sites, and these taxpayers became victims of identity theft.[48] It is understandable that some potential Free File users fall victim to scams, especially when taxpayers wishing to prepare their returns pursuant to an IRS sanctioned program visit the official IRS website only to be directed to one of 19 potentially unfamiliar commercial websites. *All taxpayers* should have the option to prepare and file their federal income tax returns *on* the IRS's own website.[49] Although Free File is accessible *through* the official IRS website, not all taxpayers are eligible to use the program. Approximately 30 percent of individual taxpayers – which amounts to more than 40 million taxpayers – are ineligible for IRS Free File.[50] Moreover, the IRS exerts little control over the content of each Free File program. As a consequence, each of the programs has its own eligibility requirements, capabilities and limitations, and the complexity is confusing to taxpayers.

Despite the IRS's best efforts, some paper filers will refuse to convert to e-file. For those cases, the IRS should develop 2-D bar code technology, which would provide

---

Gov, *IRS Free File Performance Measures - Summary View*, available at http://www.whitehouse.gov/omb/egov/c-7-3-irs.html (last visited April 7, 2008).

[47] Tax agents are regulated by the statutorily created Tax Agent Boards located in every state. For more information on the relationship between tax agents and tax administration in Australia, see http://www.ato.gov.au/corporate/content.asp?doc=/content/66215.htm (last visited March 27, 2008).

[48] *See* IRS News Release, *Late Tax Scam Discovered; Free File Users Reminded to Use IRS.gov*, IR-2007-87 (April 13, 2007). The IRS is also aware of several phishing schemes during the 2008 filing season. *See* IRS News Release, *IRS Warns of New E-Mail and Telephone Scams Using the IRS Name; Advance Payment Scams Starting*, IR-2008-11 (Jan. 30, 2008).

[49] Congress contemplated the IRS developing a basic electronic template in the IRS Restructuring and Reform Act of 1998, Pub. L. No. 105-206, 112 Stat. 685 (1998). The RRA 98 conference report states that "the conferees also intend that the IRS should continue to offer and improve its Telefile program and make available a comparable program on the Internet." H.R. Rep. No. 105-599, at 235 (1998) (Conf. Rep.).

[50] Taxpayers must have adjusted gross income of $54,000 or less to be eligible. *See* IRS Fact Sheet, *2008 IRS E-File,* FS-2008-4 (Jan. 2008); Free Online Electronic Tax Filing Agreement Amendment (2005), available at http://www.irs.gov/pub/irs-efile/free_file_agreement.pdf (last visited on April 7, 2008). Ironically, some members of the Free File Alliance provided free services to 100% of taxpayers under the initial term of the Free File Agreement and wanted to continue to do so, but the Treasury Department agreed with the Free File Alliance to place a cap on the number of taxpayers who would qualify for free tax preparation and filing services. As a consequence, Free File members are now *restricted* in the number of taxpayers to whom they may offer their services.

taxpayers and the IRS with many of the same benefits as electronic filing.[51] It is my understanding that the IRS has already incorporated this technology into other functions.

Pursuant to an Appropriations directive, the IRS Office of Electronic Tax Administration and Refundable Credits (ETA) is developing a comprehensive strategic plan to meet the 80 percent e-file goal.[52] ETA has commissioned MITRE to conduct the Advancing E-File Study, and we are pleased that the study will determine or review the following items:

- The characteristics of paper and e-filers as well as potential barriers to e-file;
- The current third-party model of tax administration and current trends in state and foreign governments; and
- Potential strategies to increase the rate of e-file or any other means to receive return information electronically. This will entail a review of direct filing with the IRS, 2-D bar coding, and Telefile.[53]

I believe this study represents an important first step in the government's fulfilling its core responsibility to taxpayers in a secure and straightforward fashion, without competing with the private sector. The Appropriations directive states that this strategic plan should be developed in consultation with me and other stakeholders, and I look forward to continuing to work with the IRS on this study.

2. The IRS Should Assert Control over its e-File Policies so that They Serve the Best Interests of Taxpayers and Tax Administration

Currently, the IRS relies completely on private industry to develop and update tax return preparation and filing software. Furthermore, when the industry encounters a problem or determines that a certain software programming update is not feasible or

---

[51] To utilize 2-D bar code technology, a taxpayer or preparer uses software to complete the return. Once printed, the return has a horizontal and vertical bar code containing tax return information. The IRS scans the return, captures the data, decodes it, and processes the return as if it had been sent electronically.

[52] Staff of H. Comm. on Appropriations, 110th Cong., H.R. 2764, Consolidated Appropriations Act, 2008, Pub. L. 110-161, Explanatory Statement at 871 (Comm. Print 2007); Staff of H. Comm. on Appropriations, 110th Cong., Financial Services and Government Appropriations Bill, 2008, at 28 (Comm. Print July 2007). Although the deadline for submission of the study was March 1, 2008, the IRS Office of Electronic Tax Administration and Refundable Credits has faced considerable challenges during the current filing season, and it is planning to complete the study later this year.

[53] Information Provided by Electronic Tax Administration (Jan. 30, 2008); Diane Freda, *IRS to Study Direct Filing Portal, 2-D Bar Coding to Boost E-Filing*, BNA Daily Tax Report (Jan. 29, 2008); MITRE IRS FFRDC, Center for Enterprise Modernization, IRS Advancing E-File Study: Draft Overview of Findings to Date (Jan. 31, 2008) (on file with the Office of the Taxpayer Advocate).

cost-effective, taxpayers and the IRS are left to deal with the downstream consequences.

The consequences of the IRS's sole reliance on the e-file industry for electronic return preparation are illustrated by a recent issue involving the economic stimulus package. Eligibility for a 2008 economic stimulus payment is based on information reported on an individual's 2007 filed income tax return. Therefore, low income taxpayers who are not typically required to file a return pursuant to IRC § 6012(a) will need to file a 2007 return in order to receive the economic stimulus payment. However, the IRS e-file systems are not programmed to accept returns reporting zero adjusted gross income (AGI). To address this limitation, the IRS quickly developed a solution that permits eligible individuals to enter $1 in AGI, without the threat of compliance-related consequences, for the sole purpose of effectuating the electronic filing of the return.[54] Yet this solution requires a certain amount of cooperation among commercial software providers due to the requisite prompts the software would need to provide the user.

The IRS has a small degree of control over Free File participants' products, but it cannot force Free File or any other software vendors to make last-minute programming changes of this nature. As of March 25, 2008, the IRS Free File webpage indicated that only five of the 19 Free File participants had accommodated the $1 work-around solution, having reprogrammed their software to alert taxpayers to this issue and directing affected taxpayers to print out step-by-step instructions to report the $1 AGI item.[55] While the IRS Free File page will seek to guide affected taxpayers to use those products that support the $1 work-around, we are concerned about the level of confusion that inevitably ensues when taxpayers without a sophisticated understanding of these issues seek to navigate the Free File site. We are also concerned about the confusion and frustration that taxpayers who do not use the Free File site encounters when they unwittingly purchase software products that do not support the $1 work-around.

The economic stimulus package as well as other late-year tax legislation presented potentially unprecedented challenges for all parties involved. The IRS was called upon to make mid-filing season systems programming changes on very short notice and managed to resolve the issues in a timely manner. At the same time, many software companies struggled to reprogram their products to accommodate the changes required by all of the late legislation. The rationale for the government's initial decision to enter into Free File and refrain from providing e-filing products itself was largely that the private sector is more innovative, nimbler, and better able to serve taxpayer needs than the IRS. However, the IRS has demonstrated this year that it *also* has the ability to rise to the occasion and meet enormous challenges on a moment's notice.

---

[54] *See* IRS Notice 2008-28, 2008-10 I.R.B. 546; Rev. Proc. 2008-21, 2008-12 I.R.B. 657.

[55] *See* http://www.irs.gov/efile/lists/0,,id=179739,00.html (last visited Mar. 25, 2008).

The 2007 filing season provided an additional example of the IRS's reactive role in the e-file arena and the resulting impact on tax administration. Taxpayers using Intuit Inc. tax return preparation and filing software products (Lacerte, ProSeries, and TurboTax) during the 2007 filing season experienced filing problems at the eleventh hour. Specifically, a significant number of taxpayers attempting to file returns through Intuit were unable to do so on April 17 (the standard April 15 deadline was extended because of a weekend and holiday) because of a slowdown in the company's electronic filing server. As a result, the IRS granted these taxpayers a two-day filing extension and agreed not to impose late-filing penalties. While the IRS and Intuit worked quickly to minimize the impact on these taxpayers, many of them still experienced unnecessary frustration and anxiety. It would be understandable if some of the affected taxpayers revert back to paper filing in 2008 – while continuing to use software to prepare their returns – after such a negative experience with the e-file process in 2007.[56]

Finally, it has come to my attention that a nonprofit-operated free return preparation and filing product faced initial opposition to its request for a listing on the IRS official website as a Free File program participant or, alternatively, as an IRS e-file partner that provides both free preparation and free filing services. The program I-CAN! E-FILE is run by the Legal Aid Society of Orange County, California (LASOC), which also happens to operate a Low Income Taxpayer Clinic (LITC).[57] The initial denial of a listing on the IRS website placed I-CAN! E-FILE in a difficult position and potentially harmed taxpayers who stand to benefit from the product, because the IRS has actively warned taxpayers about phishing schemes and informed them that the only real way to avoid becoming a victim of a potential scam is to access an e-file product through the official IRS website. Free File denied LASOC membership on two grounds: (1) membership is limited to commercial software companies, and (2) the Alliance developed its software using federal funds received through the Legal Services Corporation, a nonprofit corporation, and through the LITC grant program (which the organization vigorously disputes).[58] The IRS initially stated that

---

[56] Intuit Press Release, *Intuit Apologizes to Lacerte, ProSeries and TurboTax Customers* (Apr. 19, 2007).

[57] I-CAN! E-FILE can be used to prepare and file federal and state returns of low income taxpayers who lived and worked in one of the following states: California, Michigan, New York, Pennsylvania or Montana. The program can also add the Permanent Fund Dividend to federal returns of Alaska residents. For the 2006 tax year, the program returned more than $18,370,000 in tax refunds to 13,438 low-income taxpayers. Letter from Robert J. Cohen, Executive Director, Legal Aid Society of Orange County, to David R. Williams, Director, Electronic Tax Administration and Refundable Credits (Jan. 18, 2008) (on file with the Taxpayer Advocate Service); Letter from Robert J. Cohen, Executive Director, Legal Aid Society of Orange County, to Tim Hugo, Free File Alliance (Aug. 3, 2007) (on file with the Taxpayer Advocate Service). For more information about this product, see http://www.icanefile.org.

[58] E-mail from Robert J. Cohen, Executive Director, Legal Aid Society of Orange County, to Taxpayer Advocate Service (Feb. 29, 2008) (on file with the Taxpayer Advocate Service).

the LASOC product cannot be listed as an IRS e-file partner if the corresponding description advertises both free preparation and free filing services.[59]

When a seemingly reputable program run by a nonprofit organization has trouble obtaining a listing on the IRS website as either a Free File participant or an e-file partner merely because it is run by a nonprofit organization and wants to advertise free preparation *and* filing services in its listing description, I am concerned that the IRS's electronic filing policies have gone astray.[60] These determinations are presumably made to further the IRS e-file program, yet they do not reflect the best interests of taxpayers and do not seem to be grounded in any legitimate tax administration purpose.

I believe that the IRS should take a more proactive role in the electronic filing arena by setting the policies and standards for participation in the IRS e-file program. Such policies and procedures should align with the needs of both taxpayers and tax administration. All high quality return preparation and filing products should have equal access to the market, reflect the latest tax law changes, and be compatible with filing season peaks in demand as well as IRS's computer and processing needs. Moreover, all programs should meet IRS established minimum standards for data and identity security, and these standards should apply to both for-profit and free tax preparation offerings.[61] Unless the IRS takes corrective action, the IRS remains in a reactive position at the whim of private industry and is forced to devote scarce resources to address the downstream consequences of potentially avoidable problems. We are encouraged that the IRS is currently evaluating its role in the e-file program as part of the Advancing E-File Study and look forward to lending support to the study as well as to receiving periodic briefings of research findings as the study progresses.

---

[59] Letter from Robert J. Cohen, Executive Director, Legal Aid Society of Orange County, to David R. Williams, Director, Electronic Tax Administration and Refundable Credits (Jan. 18, 2008) (on file with the Taxpayer Advocate Service); e-mail from Robert J. Cohen, Executive Director, Legal Aid Society of Orange County, to Taxpayer Advocate Service (Mar. 5, 2008).

[60] It should be noted that exempt organizations electronically file Form 990-N, or e-postcards, for free through the Urban Institute. *See* http://epostcard.form990.org. In addition, the Urban Institute is listed as a Form 990 e-file partner with a description clearly identifying free e-file and free preparation services at http://www.irs.gov/efile/lists/0,,id=119598,00.html.

[61] At the time of this writing, it is not clear how many of the programs listed on the IRS e-file partner webpage would meet IRS-developed data or identity security specifications.

WRITTEN TESTIMONY OF DOUGLAS SHULMAN COMMISSIONER OF INTERNAL REVENUE BEFORE THE SENATE FINANCE COMMITTEE ON IRS OPERATIONS, THE FILING SEASON, THE IRS BUDGET AND IRS EFFORTS TO DEAL WITH IDENTITY THEFT

APRIL 10, 2008

Introduction

Chairman Baucus, Ranking Member Grassley, and members of the Committee, thank you for the opportunity to appear today. This is my first hearing as the IRS Commissioner, and I would like to begin this morning by thanking the Members of this Committee for their support of my confirmation. I have had productive conversations with many of you individually about the IRS and the direction we should be taking. I appreciate and value the advice and counsel that I have received, and I look forward to working closely with the Members of the Committee during my tenure with the IRS.

Because this is literally my third week on the job and because I want to make sure that, as an agency, we are as responsive as we can be to the questions you may have, I have asked Linda Stiff to accompany me this morning. Linda did an excellent job for six months as the Acting Commissioner and has helped guide the IRS on many of the filing season and economic stimulus issues that I will discuss later in my statement. She has dedicated her career to the IRS, and I am fortunate to have her support as Deputy Commissioner for Services and Enforcement.

I understand that the primary focus of this hearing is identity theft. My overall goal as the IRS Commissioner is that when a taxpayer contacts us with an issue or concern, we have in place a seamless process that gets the issue resolved promptly.

From the perspective of an identity theft victim, that means when the taxpayer calls the IRS that they reach someone who is knowledgeable on the issue and who is able to take care of the problem quickly and permanently.

Because I am new, I frankly cannot tell you this morning how far away we are from achieving that goal. I can tell you from what I have learned in the last three weeks that we are closer than we were at this time last year. I will discuss some of the things we have done in the last year later in my statement.

But before discussing identity theft in depth, I want to update you on several other items including the status of the current filing season, the distribution of the economic stimulus payments, and the President's FY 2009 Budget request for the IRS.

Overview

The IRS and its employees represent the face of U.S. government to more American citizens than any other government agency. We administer America's tax laws and collect over 96 percent of the revenues that fund the federal government each year.

The IRS strategic plan goals are:

- *Improve Taxpayer Service* – Help people understand their tax obligations, making it easier for them to comply with their obligations under the tax law.

- *Enhance Enforcement of the Tax Law* – Ensure taxpayers meet their tax obligations, so that when Americans pay their taxes, they can be confident their neighbors and business competitors are also doing the same; and

- *Modernize the IRS through its People, Processes and Technology* – Strategically manage resources, associated business processes, and technology systems to meet service and enforcement strategic goals effectively and efficiently.

The FY 2009 IRS proposed budget, which I will discuss in detail later in my testimony, supports those strategic goals by retaining the critical balance between taxpayer service and compliance and enforcement.

2008 Filing Season

The biggest challenge we faced at the end of 2007, as we approached the 2008 filing season, was the uncertain status of legislation to address the situation of an additional 21 million taxpayers who otherwise would have become subject to the alternative minimum tax (AMT).

On October 30, 2007, Chairman Baucus, Ranking Member Grassley and their counterparts on the House Ways and Means Committee, sent the IRS a letter assuring the IRS that Congress intended to enact AMT relief (the AMT patch) in a manner acceptable to the Senate, the House of Representatives, and the President. I am told that this letter was very helpful because it allowed the IRS to move forward on certain planning and design aspects of implementing the AMT relief legislation, shortening the implementation process by a number of weeks.

However, the IRS indicated that our key systems could accommodate only one programming option without introducing excessive risk to the filing season. As a result, the IRS was able to proceed only so far without actual legislation being enacted. When the President signed the AMT relief law on December 26, 2007, the IRS immediately

began the detailed reprogramming of systems to accommodate the new law. IRS employees worked diligently to modify systems to implement the changes in a very short time period. My thanks go out to all of those dedicated employees who worked almost around the clock to enable us to implement this AMT relief legislation in record time.

Given their efforts we were able to begin the filing season on schedule for most taxpayers. However, the processing of returns filed by approximately 13.5 million taxpayers that included one of five forms associated with the AMT legislation was delayed. These taxpayers had to wait until February 11, 2008, before having their filed return processed.

The other challenge facing us this filing season is the implementation of the economic stimulus package enacted in early February, specifically the planning for the distribution of the stimulus payments to eligible recipients throughout the country this spring. We will begin immediately after the close of the filing season to distribute those payments with the expectation that the first payments will be sent electronically the first week of May with the first paper checks being mailed by the second week. We have established a distribution schedule that is published on the IRS website on a page dedicated to informing citizens about the economic stimulus payments.

To deliver the 2008 stimulus payments, we must program our systems to calculate the appropriate amount for each eligible taxpayer based on their 2007 returns and then distribute the payments, through Treasury's Financial Management Service, by direct deposit or by paper check, based on the preferences expressed on their return.

However, there are a significant number of economic stimulus recipients who typically do not have an income tax filing requirement. This would include retirees or those who have minimal income and are thus not required to file. But in order to receive the 2008 stimulus payment, the recipient must file a tax return for 2007. To reach these recipients and educate them requires an extensive outreach program that includes the IRS coordinating with the Social Security Administration and Department of Veterans Affairs, along with private groups such as the AARP. We have also mailed information packets to approximately 20 million individuals who we believe may be eligible for the stimulus payment but who are normally not required to file an annual federal tax return.

Despite the challenges presented by the late enactment of the AMT patch and the implementation of the economic stimulus payments, I am proud to report that thus far the filing season has gone very well. Allow me first to give an update on some of the numbers we are looking at approximately one week from the due date for individual tax returns.

Numbers Thus Far

We expect to process nearly 140 million individual tax returns in 2008, and we anticipate continued growth in the number of those that are e-filed. In the 2007 filing season, almost 60 percent of all income tax returns were e-filed. We fully expect to exceed that

number this year. As of March 29, we have received nearly 63 million tax returns electronically, an increase of 9.3 percent compared to the number of returns that were e-filed during the same period last year.

This increase in e-filing is being driven by people preparing their own returns using their personal computers. The total number of self-prepared returns that are e-filed is up by 17 percent compared to the number of self-prepared returns e-filed during the same period a year ago. Nearly 19 million returns have been e-filed by people from their personal computers, up from just over 16 million for the same period a year ago.

Overall, 71 percent of the returns filed through March 29 have been e-filed. Encouraging e-filing is good for both the taxpayer and for the IRS. Taxpayers who use e-file can generally have their tax refund deposited directly into their bank account in two weeks or less. That is about half the time it takes us to process a paper return. For the IRS, the error-reject rate for e-filed returns is significantly lower than that for paper returns.

More people are choosing to have their tax refunds deposited directly into their bank account than ever before. As of March 29th, we have directly deposited over 50.7 million refunds, or over 72 percent of all refunds issued this tax filing season.

People are also visiting our web site – IRS.gov – in record numbers. We have recorded almost 122 million visits to our site this year, up over 19 percent from 102 million for the same period a year ago. The millions of taxpayers that have visited IRS.gov have benefited from many of the services that are available through the IRS.gov web site. The web site:

- Allows taxpayers to obtain information on the economic stimulus package including determining the payment amount that are expected to receive and learning when they can expect their payment based on their Social Security Number (SSN);

- Assists taxpayers in determining whether they qualify for the Earned Income Tax Credit (EITC);

- Assists taxpayers in determining whether they are subject to the Alternative Minimum Tax (AMT);

- Allows more than 70 percent of taxpayers the option to prepare and file their tax returns at no cost through the Free File program. This includes giving a free option for those taxpayers who normally do not file a tax return, but are required to this year in order to receive their stimulus payment;

- Allows taxpayers who are expecting refunds to track the status via the "Where's My Refund?" feature; and

- Allows taxpayers to calculate the amount of their deduction for state and local sales taxes.

We have issued $69.8 million refunds as of March 29, for a total of $172 billion. The average refund thus far is $2,467. In addition, over 26 million taxpayers have tracked their refund on IRS.gov, up nearly 20 percent over last year.

As of March 22, our Taxpayer Assistance Centers (TACs) are reporting over 1.9 million taxpayers assisted. Our telephone assistors have answered almost 12.1 million calls, and over 16 million callers received automated services.

Free File

Nearly 3.4 million people have utilized Free File as of March 29, 2008, up over 17 percent compared to the number of taxpayers that used Free File during the same period a year ago. This year anyone with adjusted gross income of $54,000 or less is eligible for Free File, which includes 97 million taxpayers. The number of Free File returns compared to the prior year has been steadily increasing, and we expect to meet or exceed 2007 totals by the end of the filing season. One reason for this increase is that we have committed additional resources to promote the Free File program.

VITA/TCE Sites and Other Community Partnerships

The use of tax return preparation alternatives, such as volunteer assistance at Volunteer Income Tax Assistance (VITA) sites and Tax Counseling for the Elderly sites (TCEs), has steadily increased over the years. In 2007, over 2.6 million returns were prepared by volunteers. As of March 30, 2008, volunteer return preparation is up almost 22 percent compared to the number of volunteer-prepared returns filed during the same period a year ago. Volunteer e-filing is also up slightly, by 2.5 percent, over the same period in the last tax filing season. This is reflective of continuing growth in existing community coalitions and partnerships.

We have also made a concerted effort to expand outreach to taxpayers, particularly those taxpayers who may be eligible for the EITC. For example, we sponsored EITC Awareness Day on January 31, 2008, in an effort to partner with our community coalitions and partnerships to reach as many EITC-eligible taxpayers as possible and urge them to claim the credit. Over 125 coalitions and partners hosted local news conferences and issued more than 100 press releases highlighting EITC Awareness Day this year.

A Commitment to Service, Enforcement and Modernization

I understand that in FY 2007, the IRS continued making improvements in our service and enforcement programs as well as having significant successes in our IT modernization program.

Taxpayer Service

According to most of our taxpayer service metrics, we continued to see improvement in FY 2007. The numbers in our telephone services, electronic filing, and IRS.gov access have all increased. This is demonstrated by the following FY 2007 business results:

- The IRS helped more taxpayers find out about their refunds through the agency's internet-based system 'Where's My Refund?' The system was accessed 32.1 million times during 2007, up 30 percent from the previous year's usage of 24.7 million.

- In FY 2007, the IRS customer assistance call centers answered 33.2 million assistor telephone calls and 21.1 million automated calls. We maintained a rating of 82.1 percent on level of service on the telephone with an accuracy rate of 91.2 percent on tax law questions.

- The agency maintained a 94-percent customer satisfaction rating for its toll-free telephone service.

- Outreach and educational services were enhanced through partnerships between the IRS and public organizations. Through its 11,922 Volunteer Income Tax Assistance and Tax Counseling for the Elderly sites, the IRS provided free tax assistance to the elderly, disabled, and limited English proficient individuals and families. Over 76,000 volunteers filed 2.63 million returns. Additionally, the IRS established 6 new tax clinics in rural areas to help low-income taxpayers meet their tax obligations.

- The IRS successfully implemented the Telephone Excise Tax Refund (TETR), a one-time payment available on federal income tax returns to refund previously collected long-distance telephone taxes. Approximately $5.48 billion was paid out in 2006 in telephone excise tax refunds. Some individual and business returns for 2006 are continuing to be filed claiming TETR refunds. In addition, the IRS prevented more than $538 million in potential erroneous refunds with the aid of a return selection tool created specifically to catch questionable TETR requests.

- The IRS also introduced a split-refund capability, which allowed taxpayers to direct deposit their refund into as many as three financial accounts.

As you know, the IRS, the IRS Oversight Board, and the National Taxpayer Advocate were charged to develop a Taxpayer Assistance Blueprint (TAB), a five-year plan that outlines the steps we should take to improve taxpayer services. As part of the implementation of TAB, the IRS has established the Taxpayer Services Program Management Office and Services Committee to provide senior executive coordination and governance to TAB implementation.

Several notable accomplishments of TAB thus far in FY 2008 include:

- Implementation of an Estimated Wait Time announcement to inform taxpayers about their expected wait time in the telephone queue prior to reaching a customer service representative;

- Implementation of Spanish "Where's My Refund," which adds refund status to the Spanish web page on IRS.gov that mirrors English-based refund information;

- Launch of an electronically searchable Publication 17, Your Federal Income Tax on IRS.gov;

- Enhanced training for volunteers in the Volunteer Income Tax Assistance (VITA) and Tax Counseling for the Elderly (TCE) programs; and

- Release of tax publications in new languages, including Chinese, Russian, Korean, and Vietnamese.

Expanding Enforcement Efforts

The most prominent measure of our success in improving compliance is the increase in enforcement revenue, which has risen from $33.8 billion in FY 2001 to $59.2 billion in FY 2007, an increase of 75 percent. These numbers do not include the deterrent effect that an increased enforcement presence has on voluntary compliance.

In FY 2007, both the levels of individual returns examined and coverage rates have risen substantially. We conducted nearly 1.4 million examinations of individual tax returns in FY 2007, an 8-percent increase over FY 2006. This is over three-quarters more than were conducted in FY 2001, and reflects a steady and sustained increase since that time. Similarly, the audit coverage rate has risen from 0.6 percent in FY 2001 to 1 percent in FY 2007. This increase was achieved without a significant increase in resources as compared to the previous fiscal year.

While the growth in examinations of individual returns is visible in all income categories, it is most visible in examinations of individuals with incomes over $1 million. Audits of these individuals increased from 17,015 during FY 2006 to 31,382 during FY 2007, an increase of 84 percent. One out of 11 individuals with incomes of $1 million or more faced an audit in 2007. Their coverage rate has risen from 5 percent in FY 2004 to 9.25 percent in FY 2007.

In the business arena, the IRS has continued efforts to review more returns of flow-through entities – partnerships and S Corporations. Our business statistics reflect that we have placed more emphasis in the growing area of these flow-through returns. While large corporate audits are down slightly, we have increased our focus on mid-market corporations – those with assets between $10 million and $50 million.

The IRS enforcement budget in FY 2007 was similar to the budget in FY 2006, and in times of flat budgets, the agency cannot increase activity across the board but must address the areas where there is growth and potential risk.

- Audits of S Corporations increased to 17,681 during FY 2007, up 26 percent from the prior year's total of 13,984.
- Audits of partnerships increased to 12,195 during FY 2007, up almost 25 percent from the prior year's total of 9,777.
- Audits of mid-size corporations increased to 4,473, up 6 percent from the prior year's total of 4,218.
- Audits of businesses in general rose to 59,516, an increase of almost 14 percent from the prior year's total of 52,223.
- Although the audits of large corporations dipped slightly in FY 2007 to 9,644 audits, the number of audits is up 14 percent from the FY 2002 level.

Finally, examinations of tax-exempt organizations have also risen. In FY 2001 5,342 tax-exempt organization examinations were closed. This number rose to 7,580 in FY 2007.

Delivering Modernization

Over the past six months, the IRS has had a number of notable accomplishments in its modernization efforts:

1. **Customer Accounts Data Engine (CADE). CADE Release 3.2** was delivered on time (January 14, 2008) for this filing season and is doing well in production. In fact, as of April 1 CADE had processed 21.96 million returns, which is more than 25 percent of all individual returns filed to date for this year. CADE has also issued almost $34 billion in tax refunds. CADE not only stores the taxpayer data on a modernized data base, but also settles daily (akin to a modern banking institution), which enables CADE to process refunds on average four days faster than the IRS master file. In addition, the updated account information is immediately available for our customer service personnel, unlike the master file, which is only updated on a weekly basis.

2. **Account Management Services (AMS).** AMS is a strategic program designed to deliver improved support and functionality to IRS employees by bridging the gap between modernization initiatives like CADE and existing legacy systems. AMS enables authorized users to access, validate, and update taxpayer accounts on demand.

   AMS Release 1.1 provides on-line address change capability for CADE accounts. The first release of AMS delivered the capability to update authoritative account data on a daily cycle to 33,539 IRS customer service representatives. Release 1.1

was deployed on time and on budget in October 2007, and through February 25, 2008, has completed over 365,000 address changes.

AMS Release 1.2 provides improved customer support with new inventory and workflow functionalities to automate the assignment, research, resolution, and closure for entity and account transcripts and transition from a paper-based manual process to an automated on-line process. Release 1.2A pilot was deployed on February 18, 2008.

3. **Modernized e-File (MeF).** MeF is the IRS' designated e-File platform (electronic filing system) for the future and provides e-Filing capability for large corporations, small businesses, partnerships, and non-profit organizations. MeF benefits both taxpayers and the IRS by enabling taxpayers to file all of their tax forms electronically, eliminating the need for IRS personnel to match paper documents to electronic returns. Additionally, the enhancements embedded within MeF allow more robust error checking and data validation before returns are processed, reducing the number of returns that need manual intervention and correction.

   As of March 31 MeF has accepted 1.5 million corporate (Form 1120), partnership (Form 1065) and tax exempt tax returns (Form 990), a 45-percent increase from this same period a year ago. MeF Release 5 went into production as planned in January 2008 and provides the ability to file electronically Form 1120F (tax returns for foreign corporations) and Form 990N (so called electronic postcard for small tax-exempt organizations to meet their filing requirement).

The President's FY 2009 Budget Funds Taxpayer Service and Enforcement

I understand that the Administration's FY 2009 Budget request for the IRS supports not only the Service's five-year strategic plan, but also the tax compliance strategies addressed in *Reducing the Federal Tax Gap: A Report on Improving Voluntary Compliance* sent to Congress last summer and the IRS *Taxpayer Assistance Blueprint.*

The FY 2009 Budget request supports improving compliance by funding activities that promote better tax administration and compliance with the tax laws. The FY 2009 Budget request for the enforcement program is $7,487,209,000, an increase of $489,983,000, or 7 percent, over the FY 2008 enacted level. The Administration proposes to include these enforcement increases as a Budget Enforcement Act program integrity cap adjustment. The enforcement program is funded from the Enforcement appropriation and part of the IRS' Operations Support appropriation.

Adjustments from FY 2008 Levels to Help Improve Voluntary Compliance

The IRS total requested funding increase for FY 2009 is $469,125,000. This increase will go to improving voluntary compliance. These investments fund increased front-line enforcement efforts, enhanced research, and implementation of legislative proposals to

improve compliance. By FY 2011, these investments are projected to increase annual enforcement revenue by $2.0 billion. In addition, the legislative proposals included in the FY 2008 Budget to improve tax compliance are estimated to generate $36 billion over the next ten years.

Specific increases to improve voluntary compliance include:

- Reduce the Tax Gap for Small Business and the Self Employed (+$168,498,000 / +1,608 FTE) – This enforcement initiative will increase enforcement efforts to improve compliance among small business and self-employed taxpayers by: increasing audits of high-income returns, increasing audits involving flow-through entities, implementing voluntary tip agreements, increasing document-matching audits, and collecting unpaid taxes from filed and non-filed tax returns. This request should generate $981 million in additional annual enforcement revenue once new hires reach full potential in FY 2011.

- Reduce the Tax Gap for Large Businesses (+$69,488,000 / +519 FTE) – This enforcement initiative will increase examination coverage of large and mid-size corporations, including multi-national businesses, foreign residents, and smaller corporations with significant international activity. It will also enable the IRS to use existing systems further to capture other electronic data through scanning and imaging. The initiative will allow the IRS to address risks arising from the rapid increase in globalization, and the related increase in foreign business activity and multi-national transactions where the potential for non-compliance is significant. Funding of this request should generate $544 million in additional annual enforcement revenue once the new hires reach full potential in FY 2011.

- Improve Tax Gap Estimates, Measurement, and Detection of Non-Compliance (+$51,058,000 / +393 FTE) – This enforcement initiative will support and expand ongoing research studies, including the National Research Program, of filing, payment, and reporting compliance to provide a comprehensive picture of the overall taxpayer compliance level. Research allows the IRS to target better specific areas of noncompliance, improve voluntary compliance, and allocate resources more effectively. Improved research data will also refine workload selection models reducing audits of compliant taxpayers.

- Increase Reporting Compliance of U.S. Taxpayers with Offshore Activity (+$13,697,000 / +124 FTE) – This enforcement initiative will address domestic taxpayer offshore activities. Abusive tax schemes, reporting of flow-through income, and high-income individuals are prime channels or candidates for tax evasion. This initiative will focus on uncovering offshore credit cards, disguised corporate ownership, and brokering activities in order to identify individual taxpayers who are involved in offshore arrangements that facilitate noncompliance. Funding of this request should generate $102 million in additional annual enforcement revenue once the new hires reach full potential in FY 2011.

- Expand Document Matching (+$35,060,000 / +413 FTE) – This enforcement initiative will increase coverage within the Automated Underreporter (AUR) program. This program matches third-party information returns (e.g., Form W-2 and Form 1099 income reports) against income claimed on tax returns. When potential underreporting is discovered taxpayers are contacted to resolve the issue. This request should produce $359 million in additional annual enforcement revenue once the new hires reach full potential in FY 2011.

- Implement Legislative Proposals to Improve Compliance (+$23,045,000 / 0 FTE) – While the IRS continues to address compliance by improving customer service and using traditional methods of enforcement, the FY 2009 Budget also includes several legislative proposals that would provide additional enforcement tools to improve compliance. It is estimated that these proposals, if enacted, will generate $36 billion in revenue over ten years (see the Treasury Blue Book, available on the Treasury Department web site, for more information). The proposals would expand information reporting, improve compliance by businesses, strengthen tax administration, and expand penalties. This enforcement initiative includes funding for purchasing software and making modifications to the IRS IT systems necessary to implement the proposals. The specific legislative proposals are discussed below.

Specific Legislative Proposals

The President's FY 2009 Budget includes a number of legislative proposals intended to improve tax compliance while minimizing the burden on compliant taxpayers as much as possible. One of the most significant of these is the requirement that there be information reporting on merchant card payment reimbursements. I was pleased to learn that that just last week the Senate Finance Committee staff released a bipartisan discussion draft of proposed legislation that included this proposal.

I appreciate the leadership that Chairman Baucus and Ranking Member Grassley have shown in supporting this important budget proposal to close the tax gap and I look forward to working with you in achieving its enactment.

Other key legislative proposals in the Administration's proposed budget:

- *Expand information reporting* – Compliance with the tax laws is highest when payments are subject to information reporting to the IRS. Specific information reporting proposals would:

  (1) Require information reporting on payments to corporations;
  (2) Require basis reporting on security sales;
  (3) Require a certified Taxpayer Identification Number (TIN) from contractors;

(4) Require increased information reporting on certain government payments;
(5) Increase information return penalties; and
(6) Improve the foreign trust reporting penalty.

- *Improve compliance by businesses* – Improving compliance by businesses of all sizes is important. Specific proposals to improve compliance by businesses would:

  (1) Require electronic filing by certain large organizations; and
  (2) Implement standards clarifying when employee leasing companies can be held liable for their clients' Federal employment taxes.

- *Strengthen tax administration* – The IRS has taken a number of steps under existing law to improve compliance. These efforts would be enhanced by specific tax administration proposals that would:

  (1) Expand IRS access to information in the National Directory of New Hires for tax administration purposes;
  (2) Permit disclosure of prison tax scams;
  (3) Make repeated willful failure to file a tax return a felony;
  (4) Facilitate tax compliance with local jurisdictions;
  (5) Extend statutes of limitations where state tax adjustments affect federal tax liability; and
  (6) Improve the investigative disclosure statute.

- *Expand penalties* – Penalties play an important role in discouraging intentional non-compliance. A specific proposal to expand penalties would impose a penalty on failure to comply with electronic filing requirements.

Improve Tax Administration and Other Miscellaneous Proposals

The Administration has put forward additional proposals relating to IRS administrative reforms. Five of these proposals are highlighted below:

- The first proposal modifies employee infractions subject to mandatory termination and permits a broader range of available penalties. It strengthens taxpayer privacy while reducing employee anxiety resulting from unduly harsh discipline or unfounded allegations.

- The second proposal allows the IRS to terminate installment agreements when taxpayers fail to make timely tax deposits and file tax returns on current liabilities.

- The third proposal eliminates the requirement that the IRS Chief Counsel provide an opinion for any accepted offer-in-compromise of unpaid tax (including interest and penalties) equal to or exceeding $50,000. This proposal requires that the

Secretary of the Treasury establish standards to determine when an opinion is appropriate.

- The fourth proposal extends the IRS authority to use the proceeds received from undercover operations through December 31, 2012. The IRS was authorized to use proceeds it received from undercover operations to offset necessary and reasonable expenses incurred in such operations. The IRS authority to use proceeds from undercover operations expired on December 31, 2007.

- The fifth proposal equalizes penalty standards between tax return preparers and taxpayers, reducing unnecessary conflicts of interest between them. The standard applicable to tax return preparers for disclosed positions would be "reasonable basis," but for certain reportable transactions with a significant purpose of tax avoidance, the existing standard would persist (i.e., the preparer should have a reasonable belief that the position, more likely than not, would be sustained on the merits).

Identity Theft

Background

Identity theft is a growing national problem. The Federal Trade Commission (FTC), the lead government agency charged with combating identity theft, has called it the number one consumer complaint in the United States. In 2006, the FTC received 246,035 complaints of identity theft.

Identity theft can affect individuals in many ways. According to the FTC, identity theft can victimize people through bank fraud, loan fraud, credit card fraud, and in many other ways. Increasingly, the victims of identity theft find that their identity is being used to allow the perpetrator to receive government benefits for which he would not otherwise be eligible. This can take the form of using identity theft to obtain a fraudulent drivers license or a government benefit to which the recipient is not entitled. It also can affect the fraudulent filing of tax returns.

Recognizing the heavy financial and emotional toll that identity theft exacts from its victims and the severe burden it places on the economy, President Bush, on May 10, 2006 created the President's Task Force on Identity Theft. This Task Force launched a new era in the fight against identity theft. It created a coordinated approach among government agencies to combat this crime by having a strategic plan that would aim to make the federal government's efforts more effective and efficient in the areas of identity theft awareness, prevention, detection, and prosecution.

In 2007, the Task Force issued a strategic report noting four major strategies for preventing and deterring identity theft. These were (1) establishing a data breach policy for the public sector, (2) improving data security in the public sector, (3) decreasing the use of social security numbers (SSNs) by the public sector, and (4) publication for a routine use with respect to disclosure of information following a data breach.

Identity Theft and Tax Administration

Generally, victims of identity theft could have their interactions with the IRS affected in two ways. First, someone could steal another person's identity and use it to file a tax return in order to fraudulently obtain a tax refund. Generally, the identity theft perpetrator will use a stolen SSN to file a forged tax return and obtain a refund early in the filing season. The rightful owner of the SSN will be unaware that this has happened until he files his return later in the filing season and we discover that two returns have been filed using the same SSN. We call this type of identity theft a refund-related crime.

The second way a person's stolen identity will affect his interaction with the IRS is if someone uses the stolen identity to obtain employment. This occurs in many instances when an undocumented worker uses someone else's SSN to get a job. In this instance, the IRS would receive a W-2 or a Form 1099 reporting income on the taxpayer's account, which the rightful owner of the SSN had not earned. Identity theft in this instance is referred to as an employment-related crime.

IRS Actions to Respond to Identity Theft

As I stated in the introduction, my overall goal as the IRS Commissioner is that when a taxpayer contacts us with an issue or concern, we have in place a seamless process that gets the issue resolved promptly. While I don't yet know how close we are to that goal, the protection of taxpayer data and other sensitive information will be a top priority during my tenure as Commissioner.

I understand that the IRS has undertaken a number of steps in the last year to both prevent and respond to incidents involving identity theft. In July 2007 the IRS created the office of Privacy, Information Protection, and Data Security (PIPDS) within the IRS.

The creation of this office recognized the importance of having an enterprise-wide approach to address identity theft problems consistently. The Director of PIPDS is a Senior Executive reporting directly to a Deputy Commissioner. This allows PIPDS to reach across all IRS organizations and ensure that proper attention and discipline is given to privacy, identity theft, and security issues.

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 identity theft issues proactively. For example, the IRS:

- Revised the most widely used documents, such as the Form 1040 instructions and Publication 17, *Your Federal Income Tax*, to include information about identity theft.

- Launched an identity theft website on IRS.gov to provide victims with updated information and links to SSA and FTC and with information on how to contact the Taxpayer Advocate.

- Participated with the Department of the Treasury and the SSA in a multi-agency panel discussion on identity theft, which was held at the IRS nationwide tax forums in 2006 that reached approximately 30,000 tax preparers.

- Developed an internal web communication tool to alert IRS employees to issues of identity theft.

- Led a multi-agency working group (Treasury, FTC, SSA, and Homeland Security) with a goal of providing consistent information and services to victims, consistent with recommendations being made by the President through the Identity Theft Task Force.

- Promoted a consistent message to inform taxpayers that the IRS does not communicate with taxpayers via e-mail, with the goal of reducing the number of identity thefts accomplished by "phishing."

- Published, jointly with the Treasury Inspector General for Tax Administration (TIGTA), an e-mail address on IRS.gov to serve as a repository for the fraudulent emails so they could be tracked to the source and destroyed, and if appropriate referred for criminal action.

Victim Assistance

The IRS recognizes that outreach alone is not enough and that it also must be prepared to assist victims when identity theft occurs.

- In January 2008, the IRS implemented a new service-wide identity theft indicator that is placed on a taxpayer's account upon the authentication of identity theft. All applicable IRS functions are now tracking tax fraud identity theft victims using the universal identity theft indicator. Since January, indicator s have been placed on more than 3,000 accounts. This new process means that taxpayers should only have to provide identity theft authentication one time.

- Beginning in January 2009, returns filed using SSNs associated with accounts that are coded with a universal identity theft indicator will be filtered to distinguish legitimate returns from fraudulent ones. In this way, the universal identity theft indicator will reduce taxpayer burden and inconvenience by expediting the process for identifying and processing the victim's return.

- The IRS established a new identity theft policy that provides for more consistent procedures across its functions to ensure timely resolution of identity theft issues affecting taxpayer accounts.

- The IRS has developed new standards for documentation required from taxpayers to validate the identity of the taxpayer and the fact of the identity theft. For example, taxpayers can now fax information to the IRS that verifies their identity rather than appearing in person at an IRS office. These documentation standards are consistent with those required by FTC and SSA.

- The IRS is now able to resolve approximately 95 percent of all duplicate match cases through research and input from the taxpayer. In the other 5 percent of the cases where the IRS cannot easily determine which party is the legitimate owner of the SSN, we must engage in more rigorous procedures including the involvement of SSA to resolve the case. The IRS recognizes that more work is needed to reduce the burden placed on legitimate taxpayers whose cases are not easily resolved.

- In September 2007, the IRS began sending letters to individuals affected by IRS data loss incidents (e.g., lost or stolen laptops or tax returns lost in shipping). While these incidents are not wide-spread, the notification letter to those that are affected includes an offer for one-year free premium credit monitoring that includes credit monitoring, identity theft insurance up to $20,000, and 24/7 fraud victim assistance. To date, approximately 10 percent of notified individuals have taken advantage of the credit monitoring service, which is consistent with the industry standard.

Prevention

The IRS is also working to prevent identity theft:

- The IRS' Criminal Investigation (CI) division initially identifies many cases of identity theft through its Refund Crimes Unit. This includes instances where a criminal uses another person's tax information to fake a return and steal a refund. CI identifies questionable tax returns using the Electronic Fraud Detection System (EFDS). EFDS screens tax returns, and if certain indicators of fraud are discovered the refund becomes part of the Questionable Refund Program (QRP). In Tax Year (TY) 2007, the IRS identified over 240,000 fraudulent returns and stopped over $1.2 billion in fraudulent refunds from being made. Of this total, identity theft was suspected in approximately 27,500 returns.

- The IRS is working with the SSA to reduce the incidence of identity theft related to employment by improving the accuracy of SSN reporting.

- The IRS is implementing recommendations from the President's Identity Theft Task Force strategic report and in accordance with an OMB directive to reduce or eliminate the use of SSNs within Federal agencies.

- The IRS has created new specialized personnel positions for detecting and preventing online fraud.

Other Identity Theft-Related Initiatives

- **IRS Efforts to protect personal information for taxpayers interacting with the IRS electronically** – The IRS is continually exploring ways to ensure taxpayers who e-file or seek tax help through IRS.gov or other online tax-related services can be assured their information is safe. We are also working to put in place mechanisms to prevent the use of stolen identities to file electronically. We are also working to promote a comprehensive online fraud awareness, training, and education program within the public and private sectors to reduce vulnerabilities and minimize online fraud.

  The IRS is the 24th most "spoofed" brand in the world according to an October 2007 report. Spoofing means to use the brand in such a way as to make the individual think that he is coming to a site owned by the real owner of the brand – such as the IRS. To combat phishing efforts spoofing the IRS brand and other tax-related web sites (e.g. tax preparation services), we identified and took down nearly 900 phishing sites last year and have already taken down half that number in the first two months of 2008.

- **Refund Crime Notification Pilots** – In February 2008, the IRS began a notification pilot for individuals whom CI has identified as identity theft victims of traditional refund crimes. In these cases, the perpetrator uses the victim's personally identifiable information (PII) to fabricate a return. The letter to the taxpayer provides that: (1) someone may have attempted to impersonate you by using your personal information; (2) we have adjusted your account to reflect the corrected tax return information; (3) we suggest you monitor your financial accounts; and (4) includes information on how to obtain identity theft assistance.

Identity Theft and the Economic Stimulus Payments

Earlier in my statement, I spoke of the progress we have made in preparing to issue the economic stimulus payments beginning in early May. However, the stimulus program poses some unique challenges directly related to identity theft.

Specifically, in order to receive a 2008 stimulus payment the recipient must have filed a 2007 tax return. This means that millions of senior citizens, railroad retirees, and others who are not normally required to file returns must do so for 2007 in order to receive their stimulus payments. IRS has an aggressive outreach program in place to contact these citizens to let them know that they must file a return to get their stimulus payment.

However by law, all advance stimulus payments must be issued by the end of 2008. Therefore, a victim of identity theft may not be able receive the economic stimulus payment because an identity thief has already filed a return using that individual's personal information and received the payment.

In these instances, it is critical that the case be resolved quickly so that the appropriate party can get the stimulus payment by the end of the year. This scenario could apply to individuals who otherwise have a filing requirement as well as to individuals who do not. Therefore, IRS is expediting procedures to resolve instances of identity theft related to stimulus payments.

We have created a specialized group of assistors to speed the processing of economic stimulus payments affected by identity theft. We have in place streamlined processes for proof of identity and proof that the identity has been stolen. We are working to develop treatment procedures for victims whose economic stimulus payments are affected by identity theft.

Conclusion

Thank you again, Mr. Chairman, for the opportunity to appear this morning and update the Committee on the filing season, IRS Operations, the FY 2009 proposed IRS Budget, and our efforts on identity theft. In my short tenure, I have found IRS employees to be professional, hardworking, and dedicated.

Despite any progress that we make, I understand that we must continue to work hard everyday to provide taxpayers the high level of service they deserve and to pursue enforcement actions against those unwilling to meet their tax obligations.

The identity theft issue is a good example. We have made progress, but we know we still have work to do. We recognize that we need to strive constantly to improve the policies, processes, and procedures for assisting identity theft victims. And, we have taken steps to develop a more consistent, more efficient, and less burdensome manner for handling identity theft cases.

We also need the resources to do our work. I hope this Committee will support the full funding of the Administration's FY 2009 proposed budget. It will enable us to build on the programs we have started in the past.

I also urge this Committee to support the enactment of the legislative proposals included in the Budget to improve compliance. Collectively, they will generate more $36 billion over the next 10 years if enacted.

Linda and I will be happy to respond to any questions.

SENATE COMMITTEE ON FINANCE
HEARING ON
"Identity Theft: Who's Got Your Number?"
April 10, 2008

Questions for Commissioner Douglas H. Shulman

Questions from Chairman Baucus:

1. **At the hearing, you made a commitment to look at the IRS identity theft strategy in a comprehensive manner and to provide a report to me within 90 days. I look forward to receiving that report. In addition, you indicated you would report back within 2 weeks of the hearing to provide a specific date by which the IRS's identity theft team would be up and running. Please specify the date that the ID theft team will be fully operational and available to provide services to taxpayers.**

   Since the hearing, I have asked my staff to provide an update on the IRS' updated identity Protection Strategy to the Committee. We provided that update to the Committee on July 21, 2008. The report highlights IRS' focus on actions to combat tax-related fraud and to assist taxpayers who are identity theft victims, through a combination of prevention and assistance activities. The Identity Protection Strategy is built upon three overarching priority goals: Victim Assistance, Outreach and Prevention.

   On October 1, 2008, the IRS opened a specialized unit dedicated to resolving tax issues incurred by identity theft victims. This unit will enable victims to have their questions answered and issues resolved quickly and effectively. Victim assistors will handle taxpayer inquiries from multiple sources including a dedicated identity theft telephone line. We will begin with between 30 to 60 people staffing the telephones in up to four IRS locations nationally and will add more assistors depending on the volume of requests for assistance. To ensure we can address additional paper and telephone inquires, we have trained a total of 161 IRS assistors to handle telephone inquiries in both English and Spanish and 71 assistors to address the paper inventory. The telephone inquiry services will operate from 8:00 a.m. to 8:00 p.m. with Hawaii and Alaska following Pacific Standard Time.

   We will ensure that identity theft issues are resolved by preparing our employees with the expertise to address each issue. Our goal is to resolve issues promptly and permanently.

2. **Mr. Shulman, your written testimony states it is your goal that when a taxpayer contacts the IRS with an identity theft issue or concern, the IRS will have a "seamless process" in place to resolve the issue promptly. You also state that you "frankly cannot tell [me] how far away [the IRS] is from achieving that goal."**

   In 2005, and again in a report released on April 9, 2008, TIGTA put the IRS on alert that it lacks an adequate corporate strategy to address identity theft issues. The Taxpayer Advocate has reported similar concerns for the last several years. Last year, this Committee listened to a convicted identity thief describe how easy it

was to file false tax returns using stolen identities. This is not a new problem. Yet, the IRS does not know how soon a seamless process will be in place.

a. Why not? Describe why the IRS has failed to implement an effective agency-wide strategy that will deal pro-actively with identity theft issues, and why it is taking so long to achieve.

In 2004, the IRS recognized identity theft as a growing problem and addressed the challenge through the development of an enterprise strategy. This strategy has evolved and will continue to serve as the foundation for all of our efforts to provide services to victims of identity theft and to reduce the effects of identity theft on tax administration. The original strategy and our recent July 2008 update focus on three priority areas that are fundamental to addressing the identity theft challenge: Victim Assistance, Outreach, and Prevention.

- **Victim Assistance**: Assist taxpayers with resolving tax issues that arise from identity theft as quickly as possible and with minimal disruption.
- **Outreach**: Increase taxpayer awareness of identity theft through multiple communication channels and education efforts.
- **Prevention**: Build a strong prevention program to significantly reduce incidents of identity theft and protect the American taxpayer.

The IRS strategic plan reinforces the priorities of the Identity Protection Strategy with parallel goals including a goal to ensure seamless taxpayer service by fostering IRS employee ownership of taxpayer issues. We believe that significant progress has been made to date but recognize that there is still work to be done.

b. Why hasn't the IRS put a higher priority on a problem that takes such a financial and emotional toll on its victims?

We have made significant progress in each of the priority areas of the strategy and are committed to continuing efforts to reduce the burden on taxpayers who have become victims of identity theft.

In July 2007, the IRS formed a new office, the Office of Privacy, Information Protection and Data Security (PIPDS), dedicated to privacy and the protection of information. PIPDS is led by an experienced Senior Executive who reports directly to the Deputy Commissioner for Operations Support, which enables the office to reach across all IRS organizations and ensure that proper attention and discipline are given to the issues of privacy, identity theft and data security. PIPDS collaborates with business units across the IRS to develop holistic solutions to assist the victims of identity theft. Over the last year, this office has more than doubled its resources dedicated to privacy and identity theft issues as a result of the IRS' heightened emphasis on identity theft.

The IRS has established the Online Fraud Detection and Prevention (OFDP) office within PIPDS to address the increasing and evolving threat of online fraud affecting the IRS and taxpayers. The mission of this office includes:

- A rapid response capability to detect and mitigate against online fraud incidents;
- A robust analytic and operational information sharing capability to prevent and reduce risk;
- Use of technological innovations and process improvements to tackle current and next generation online fraud schemes; and
- Comprehensive online fraud awareness, training and education programs with public and private sectors to reduce vulnerabilities and minimize the severity of online fraud.

IRS Criminal Investigation (CI) Division and the OFDP office are working closely with the Treasury Inspector General for Tax Administration (TIGTA), the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI) and the Federal Trade Commission (FTC) to pursue criminal investigations as appropriate.

In January 2008, the IRS began using an indicator to mark identity theft cases, and all IRS functions updated their Internal Revenue Manual procedures on the application and use of the indicator. In October 2008, we began using the indicator to mark taxpayers' accounts where they have self-reported incidents of identity theft that have not yet affected their tax accounts. In January 2009, we will use the indicator to assist in distinguishing legitimate returns from fraudulent returns submitted by identity thieves.

As we stated in our response to Question 1, the specialized unit opened on October 1, 2008. Taxpayers can reach the unit through a dedicated toll-free identity theft telephone number at 800-908-4490. Additional information on the specialized unit and how taxpayers can prevent identity theft is available on IRS.GOV using the key word, "identity theft".

3. **Please comment on each of the following suggestions from Ms. Spencer, Ms. Olson and Mr. George on ways the IRS can more effectively deal with identity theft.**

   - **An overarching IRS office that is responsible for tracking and resolving identity theft cases for all types of taxpayers. Even if other functions were involved, this office would ultimately be accountable to monitor the cases and ensure they were resolved satisfactorily.**

     The IRS opened a specialized unit on October 1, 2008, to provide taxpayers with a central point of contact for the resolution of tax issues caused by identity theft. This unit will provide end-to-end case resolution. Victims will be able to communicate with one customer service representative to have their questions answered and issues resolved quickly and efficiently. In addition, the new unit will support victims by simplifying the process for verifying their identity and the occurrence of identity theft. These new services and procedures will reduce taxpayer burden related to identity theft.

   - **A way for taxpayers to notify the IRS *before* identity theft crime turns into a tax crime.**

In October 2008, we began offering taxpayers the opportunity to self-report incidents of identity theft that have not yet affected their tax accounts.

- **Notifying taxpayers when other individuals use their social security numbers in connection with a tax matter.**

  We are currently developing letters to notify taxpayers when the IRS discovers that other individuals are using the taxpayer's name and Social Security Number (SSN) for tax administration purposes. For example, we have recently issued letters to taxpayers when someone has attempted to impersonate them by using their personal information to file a tax return. In addition to notifying these taxpayers, we provide them with the information and resources that they need to resolve their tax-related issues and to prevent future harm.

- **Notifying taxpayers when their refunds are frozen in connection with an identity theft matter.**

  When both the identity thief and the rightful taxpayer file tax returns, this creates a duplicate filing condition. Both refunds are frozen in these instances until we can distinguish the true owner of the SSN. We do this to protect the taxpayer and the integrity of tax administration to ensure that the legitimate taxpayer's refund and tax information are not erroneously released to the identity thief.

  Most duplicate returns filed using the same SSN do not involve identity theft and are quickly resolved. The IRS first tries to determine whether there is another reason for the duplicate filing, such as transcription errors, a single taxpayer filing multiple returns for the same year to correct mistakes, or the most common cause, transposition errors by the taxpayer. If we still cannot determine why we have received duplicate returns, the IRS contacts the taxpayer to request additional information. We then send a letter to the taxpayer to notify them that their refund has been frozen until we resolve the true ownership of these returns.

  The IRS is chartering a cross functional team including subject matter experts from Wage and Investment, the Taxpayer Advocate Service and PIPDS to evaluate duplicate filing cases where there is a substantial delay to identify further process improvements.

- **Empowering IRS employees to make common sense decisions when the true owner of an SSN is obvious.**

  We are currently taking actions to improve our duplicate filing processes to enhance the resolution of cases that may be connected to identity theft. Our goal is to develop guidelines to assist our employees in determining the true owner of the SSN in duplicate filing instances. Specifically, in June 2008, we chartered a Lean Six Sigma team to conduct a comprehensive analysis of the duplicate filing process/procedures and to make formal recommendations for improvements. In fact, we are currently testing these guidelines to determine their effectiveness.

  One of the outcomes anticipated from the various improvement initiatives are guidelines for how an IRS employee can distinguish the true owner of an SSN from

an identity thief. The team is scheduled to report the findings and proposed recommendations for solutions in the Fall 2008.

4. **In 2006, the IRS spent $21 million on a system to detect filing fraud that failed and had to be abandoned. To what extent are existing IRS filters adequate to catch identity theft? What is the status and timeline of IRS plans to develop a new electronic filing fraud system?**

   The IRS uses a variety of filters to detect filing fraud and catch identity theft. We apply these filters when we receive tax returns to detect those returns with questionable characteristics. Additional error resolution procedures are applied to these questionable returns before they are processed. For example, if the combination of the name and SSN used on the return does not match our records, we will not process the return until this inconsistency is resolved.

   In addition, the IRS' CI Division uses the Electronic Fraud Detection System (EFDS) to screen questionable returns and identify schemes involving identity theft. We have developed new filters to identify new crimes as the techniques used by identity theft criminals evolve. For example, we developed a filter to identity those returns that have been stolen by a perpetrator through a phishing scheme.

   The Fraud Detection Centers (FDCs) within our CI Division continue to improve our processes for identifying and analyzing fraudulent tax refund schemes involving identity theft. The FDCs forward those returns meeting the appropriate criteria to our field investigation offices to develop potential recommendations for prosecution. Beginning in January 2009, we will use the identity theft indicator to assist in distinguishing legitimate returns from fraudulent returns submitted by identity thieves.

5. **How many dollars did the IRS send out in erroneous refunds related to identity theft during filing season 2008?**

   For the filing season 2008 and as of October 8, 2008, Criminal Investigation identified over 341,000 fraudulent returns and stopped over $1.5 billion in fraudulent refunds. Identity theft was suspected in approximately 27,500 of these fraudulent returns. Refunds stopped on the suspected identity theft returns was approximately $151 million and refunds lost was approximately $13 million.

6. **Ms. Spencer testified that her client made contact with at least four IRS functions to resolve her identity theft dispute.**

   a. **Explain why the IRS does not have a one-stop office that can handle these cases? How many different IRS departments deal with tax related identity theft?**

      We opened a specialized unit on October 1, 2008, to provide taxpayers with a central point of contact for the resolution of tax issues caused by identity theft. We have found that, over time, identity theft cases can be handled by approximately 24 functional areas of the IRS, including customer service, tax return processing, and compliance, and we believe this new unit will assist taxpayers whenever the need arises in dealing with identity theft.

b. Explain why the IRS refused to give Ms. Spencer's client a transcript of her own tax account. Aren't taxpayers entitled to see what's going on with their own account?

With few exceptions, Section 6103 of the Internal Revenue Code permits the release of return information only to the owner of that return information. In accordance with this provision, the IRS requires that taxpayers verify their identity through a clear authentication process prior to the release of the tax account transcripts. The IRS regularly provides transcripts to those taxpayers who have verified their identities.

We have been in contact with Ms. Spencer's client to identify the reason why her client was not able to timely receive an account transcript. We will continue to consult identity theft victims to seek advice on ways to improve our services.

7. If I discover that I am a victim of identity theft, I want to let the IRS know about it as soon as possible. When I go to the IRS website, I am told I need to file a complaint with the Federal Trade Commission. There's also a toll free IRS number listed. Yet, according to the TIGTA report released on April 9, 2008, the IRS does nothing with the FTC data. And when I call the toll-free number, there is no mention of what to do about cases of identity theft.

a. Why doesn't the IRS have a mechanism in place to allow identity theft victims to notify the IRS right away - before they have tax troubles - to put a flag on their account?

The new identity protection specialized unit opened on October 1, 2008, and we offer taxpayers the opportunity to self-report incidents of identity theft that have not yet affected their tax accounts. Taxpayers can reach the unit through a dedicated toll-free identity theft telephone number at 800-908-4490.

b. To what extent is it misleading to direct victims to the FTC website when the IRS does not coordinate with the FTC? Wouldn't victims assume the IRS is going to use that information to protect their accounts? What plans does the IRS have to start using the FTC data?

The IRS receives data from the FTC relating to identity theft, and we continue to partner with the FTC and other Federal agencies to evaluate the FTC data to identify current identity theft trends. We use this information to provide clear and consistent guidance to taxpayers about identity theft.

CI evaluates and employs a wide variety of information sources to identify potential identity theft fraud and to support recommendations for prosecutions. This includes data from various state, federal and local law enforcement agencies that investigate identity theft crimes. CI was able to use these sources to identify 7,000 cases over and above the 20,000 cases reported to the FTC in 2007.

The IRS collaborates with the FTC to provide taxpayers with up-to-date information on identity theft. This information includes best practices for protecting personal information, reporting identity theft crimes and recovering their identity. For example, the IRS partners with the FTC and other government agencies to maintain

OnGuardOnline.gov. OnGuardOnline.gov provides practical tips on avoiding internet fraud, securing your computer and protecting personal information.

8. **In my opening statement, I described how some IRS processes actually appear to facilitate identity theft. These involve returns filed by persons using Individual Taxpayer Identification Numbers – or ITINs – who attach W-2s to their returns with other persons' social security numbers. That's a red flag that something might be wrong. According to IRS statistics, over a million returns were filed in 2005 using ITINs. The IRS told TIGTA it does not plan to more actively try to identify or stop individuals from committing employment-related identity theft. Please explain why the IRS does not consider it to be the agency's responsibility to prevent continued tax related identity theft. Why won't the IRS flag the social security number holder's account or notify the victim that someone appears to be using his number?**

All employment related identity theft may not result in the requirement to file a tax return. Given the broader nature of identity theft crimes, the President's Task Force on Identity Theft has directed the DHS the lead Agency to address targeted enforcement initiatives for this type of employment related crime.

By law, all taxpayers must have an identifying number (Taxpayer Identification Number) for themselves, spouses, and dependents required to be listed on any return, statement, or other document that they must file under the Internal Revenue Code. Any taxpayer eligible for an SSN must provide an SSN as this identifying number; however, not all taxpayers who have a U.S. tax or reporting obligation qualify for an SSN. This happens when foreign investors and persons working in the United States without authorization have U.S.-source income equal to or in excess of the exemption amount. Furthermore, while the Code differentiates between resident and non-resident alien, it offers no distinction based upon whether a resident alien is legally present in the United States. When resident aliens are legally required to file and pay U.S. taxes, the IRS must provide an alternate to the SSN, such as an ITIN to be used as an identifying number on returns, statements and other documents related to that obligation regardless of whether an SSN was used illegally to obtain employment.

Following the end of each calendar year, the Social Security Administration (SSA) receives wage information submitted by employers on W-2s. SSA credits these wages to the records of individual workers that it maintains for social security program purposes. In order for the wages to be credited to an individual worker, the worker's name and SSN reported by the employer on the W-2 must match the name and SSN recorded in SSA's records of assigned Social Security Numbers. The W-2s in which the name and SSN match those on SSA records are credited to the earnings records of individual workers. For W-2s where the submitted name and SSN do not match SSA records, SSA undertakes various activities to obtain a match. First, SSA uses a number of software routines on the submitted information to obtain a name/SSN match. If these routines do not result in a match, SSA attempts to resolve the mismatched items by sending "no match" letters to inform individuals that the information reported to SSA does not match SSA records. SSA's goal is to credit wages reported on W-2s to the record of the worker who earned them.

The SSA offers employers the online Social Security Number Verification Service (SSNVS) to verify that their employees' names and SSNs match SSA's records.

E-Verify is an online system administered by the Department of Homeland Security (DHS) with support from SSA. Participating employers can check the employment eligibility of new hires online by comparing information from an employee's I-9 form against DHS and SSA databases. More than 69,000 employers are enrolled in the program, with over 4 million queries run so far in fiscal year 2008. SSA's OIG will assist DHS in worksite enforcement matters on a case-by-case basis. In addition, the IRS is actively engaging both the SSA and the DHS to collaborate on strategies to mitigate the effect of employment related theft on victims.

As we partner with other agencies to combat the effects of identity theft crimes, the IRS is currently reviewing the disclosures we are permitted to make under current law in identity theft cases. To that end, we have formed a working group representing several IRS offices and divisions to review the IRS' existing disclosure authority and to explore the issues surrounding what types of information can be shared with external parties.

9. **TIGTA reports that IRS policy is that the actual crime of identity theft will be investigated by the IRS only if it is related to a more serious offense. Some victims suffer the same tax problems year after year because the IRS does nothing to stop the identity thief from repeating his crime. Last year, former Commissioner Everson told this committee that identity theft cases involving less than $40,000 would not be prosecuted due to lack of resources.**

   a. **To what extent do you agree with this policy? How should it be changed?**

      The IRS makes recommendations for prosecutions based upon the merits of each case. The Department of Justice (Tax Division) and the United States Attorney's Office have sole discretion over what charges will be brought in a fraudulent refund case.

      The IRS makes recommendations to prosecute identity theft cases that have a nexus to a tax crime. Not all identity theft cases have this associated nexus. As recommendations are made for prosecution of identity fraud using several statutes within our jurisdiction, the use of Title 18 USC § 1028 is recommended to enhance egregious cases where tax or money laundering violations are being charged.

      The IRS is limited in our ability to pursue identity theft cases under Title 18 USC § 1028A, the "aggravated identity theft" statute. This statute adds additional penalties for convictions where identity theft has been used as a step in committing one of the felony violations specified in Section § 1028A. This statute is of limited use to the IRS because the felony convictions under this statute do not include any Title 26 tax-related offenses; any Title 18 USC §§ 286/287 false claims offenses; or any Title 18 USC §§ 1956/1957 money laundering offenses.

      Despite these limitations, over the past three years, the CI Division has investigated a number of tax-related identity theft cases that the Department of Justice successfully prosecuted. For example, a former Girl Scout troop leader, Holly Barnes, in the Florida Panhandle is now serving ten years in federal prison for using the children's identities to defraud the government. Barnes pleaded guilty in October 2007 to multiple counts of filing fictitious tax claims and identity theft. Barnes created fake medical release forms for her troop members and told their parents that she

needed the girls' Social Security numbers in case of an emergency. The scheme helped her claim more than $87,000 in fraudulent tax refunds.

b. Does the IRS have sufficient resources to adequately pursue identity theft cases?

i. If so, why is the IRS's identity theft strategy inadequate?
ii. If not, what is an appropriate level of resources and what actions do you intend to take to secure those resources?

In recent years, the IRS has devoted increased resources to detecting and investigating identity theft tax fraud. Our Special Agents in CI regularly collaborate with other enforcement agencies, such as the FBI, the United States Secret Service (USSS), the United States Postal Inspection Service (USPIS), the SSA Office of the Inspector General (OIG) and the DHS to investigate identity theft cases.

The IRS FDCs within the CI Division continue to improve ways to identify and analyze fraudulent tax refund schemes involving identity theft. Those returns meeting the appropriate criteria are forwarded to our field investigation offices to develop potential recommendations for prosecution.

c. What are the opportunity costs to the IRS because it has not taken a more proactive approach toward identity theft? What else could the IRS be doing with the resources it spends on identity theft related tax problems that could be prevented by earlier notification or by not having to deal with the same victims year after year?

The IRS is, and has been, taking a more proactive approach to identity theft. One of our primary goals has been to streamline processing of identity theft tax problems. For example, before the implementation of the enterprise identity theft indicator, the Automated Underreporter (AUR) function had developed its own indicator to help stop subsequent year contacts when a taxpayer had established identity theft. While this effort had already contributed to some reduced work, and the new centralized assistance unit is expected to handle taxpayer contacts efficiently, we are expending additional resources in the implementation of a new identity theft indicator, return filters, and return screening. These efforts illustrate the redirection of resources to overall program improvement.

We use the identity theft indicator to mark the taxpayer's account and to prevent victims from encountering the same problems year after year. We will use this indicator in our screening process and compare the characteristics of the file return with the historical filing characteristics of the taxpayer. Our employees will review suspicious accounts and interact with the taxpayer to verify that a legitimate return was submitted by the taxpayer.

Additionally, we are currently testing a process to notify individuals the IRS has identified through its research as identity theft victims of traditional refund crimes (i.e., when the perpetrator uses the victim's personal information to fabricate a return) or of online phishing refund crimes (i.e., when a perpetrator intercepts a legitimate online tax return and alters the bank account to reroute a refund).

d. What can the IRS do to prevent victims from encountering the same problems year after year because someone else repeatedly uses their identity?

In January 2008, the IRS began using an indicator to mark accounts of taxpayers that have been victims of identify theft. This indicator will be used to prevent victims from encountering the same problems year after year.

10. In both your oral and written testimony you discussed a new IRS team of employees who will be specially trained to handle identity theft that will be up and running by this fall. What type of special training will these employees receive and what will be their roles and responsibilities?

We are currently training experienced Customer Service Representatives (CSRs) as victim assistors in the identity theft specialized unit. Their primary role will be to answer phone calls and correspondence from identity theft victims. Some of these contacts may result in complete resolution upon initial contact by the taxpayer. However, for those which do not result in immediate resolution, the CSRs may need to engage other expert IRS resources to resolve all of the taxpayer's issues and complete the case. The CSR will have the responsibility to ensure the marker is applied to the account and to monitor the taxpayer's cases to make certain the issues are resolved quickly and completely.

Will these employees be able to handle all aspects of a case involving identity theft, or will taxpayers and their representatives still have to deal with other areas of the IRS to resolve their cases?

Each CSR has ultimate responsibility to provide seamless service and ensure their taxpayer's case is resolved quickly and completely. This an example of how we are delivering our IRS strategic goal of ensuring seamless taxpayer service by fostering employee ownership of taxpayer issues. The CSRs may need to engage additional IRS experts to resolve complex issues or execute complex account adjustments.

What functions will the staff be pulled from and what will be the effect on the operations of those functions losing staff or having staff diverted from their normal tasks?

The specialized identity theft victim assistance unit will be staffed with experts including CSRs from the Accounts Management function of Wage and Investment Customer Accounts Services. The overall resource impact of staff diversion should be minimal.

11. Describe to what extent the IRS is working with the National Taxpayer Advocate to develop the IRS identity theft strategy, including the security of taxpayer data. Describe how the IRS evaluates the NTA's recommendations and determines whether to adopt them.

The IRS is working closely with the Taxpayer Advocate Service (TAS) to develop the IRS Identity Protection Strategy and procedures to resolve the issues identified in the TAS 2007 Annual Report to Congress (ARC). We engaged the TAS to develop solutions collaboratively to address all eight identity theft-related concerns identified by the National Taxpayer Advocate in the 2007 ARC. For example a cross-functional team of IRS and TAS employees are developing procedures for the specialized unit and the

process for taxpayers to self-report incidents of identity theft that have not yet affected their tax administration accounts.

The Executive Director, Systemic Advocacy within the TAS participates as a voting member in the Identity Theft and Incident Management (ITIM) Advisory Council. This Council provides oversight of effective policies and procedures to protect personal information and resolve cases of identity theft.

12. **The Advocate has made a number of suggestions that would allow taxpayers to proactively notify the IRS when they believe they have been a victim of identity theft. Is the IRS considering developing a mechanism by which a taxpayer can notify the IRS upon discovery that he may be the victim of identity theft?**

Yes, we offer taxpayers the opportunity to self-report incidents of identity theft that have not yet affected their tax accounts beginning in October 2008.

Is the IRS considering allowing taxpayers to block electronic filing of tax returns using their SSN?

Given the benefits of electronic filing, and the volume of account-related contacts that would be needed to unblock filings each year, we believe this proposal would be more burdensome for taxpayers than the development of IRS screens and filters that will accomplish the same effect. We are concentrating our improvements for the electronic filing of tax returns on making e-file smarter in order to block more effectively the criminals from committing electronic tax fraud. This includes evaluating additional enhancements to e-file security and functionality. We believe that we can provide the best taxpayer service by focusing on preventing perpetrators from filing fraudulent returns rather than reducing electronic services and increasing taxpayer burden.

13. **Describe to what extent the IRS is working with the Treasury Inspector General for Tax Administration to develop the IRS identity theft strategy, including the security of taxpayer data. Describe how the IRS evaluates the TIGTA's recommendations and determines whether to adopt them.**

Over the last year, the IRS has been working collaboratively with the Treasury Tax Inspector General for Tax Administration (TIGTA) on a number of initiatives including the development of processes to reduce online fraud. The OFDP office works closely with the TIGTA to address the increasing and evolving threat of online fraud. For example, the OFDP office and the TIGTA have developed a rapid response capability to detect and mitigate against online fraud incidents. These offices also share a robust analytic and operational information sharing capability to prevent and reduce risk.

The IRS agreed with, and has taken steps to pursue aggressively, the formal TIGTA recommendations with respect to the protection of taxpayer data. These efforts have significantly influenced the development of IRS' updated Identity Protection Strategy.

14. **Both TIGTA and the National Taxpayer Advocate have recommended that the IRS make the PIN process mandatory for all electronic filers. To what extent does the IRS have any plans to implement this recommendation?**

Beginning January 1, 2009, the IRS will require a PIN to process all electronic returns. Taxpayers will no longer be able to submit a hand written signature using form 8453-OL.

15. Your written testimony states that in January 2008, the IRS implemented a new, service-wide identity theft indicator that is placed on a taxpayer's account upon the *authentication* of identity theft [emphasis added]. Please describe what constitutes "authentication" – under what circumstances will the indicator be used?

Authentication of identity theft requires proof of identity (government issued identification such as a driver's license or passport) and proof of theft (a police report or FTC identity theft affidavit). The identity theft indicator will be used to mark taxpayers' accounts once they have verified their identity and the occurrence of an identity theft when there as been a tax administration effect. Beginning in October 2008, we offer taxpayers the opportunity to self-report incidents of identity theft that have not yet affected their tax accounts. The same two pieces of information will be used to substantiate self-reported incidents of identity theft.

How effectively will this process be able to identify and quantify all taxpayer cases associated with identity theft?

The identity theft indicator is an effective tool in addressing identity theft because it is available to all employees who provide assistance to taxpayers. For the first time, there is a standard, enterprise-wide indicator that IRS employees can use to recognize identity theft cases easily and monitor their resolution.

How does the new identity theft indicator work?

The IRS began using an indicator to mark identity theft cases in 2008 and will use the indicator in 2009 to identify suspicious return filings. Please see our response to Question 9 for additional details about how the identity theft indicator works.

How long will the indicator remain on the taxpayer's account?

The indicator will remain on the taxpayer's account for 3 years.

What guidance has the IRS issued to employees regarding the indicator and how it will function?

The IRS Deputy Commissioner for Operations Support and Deputy Commissioner for Services and Enforcement issued a memorandum to explain the purpose and use of the indicator in June 2007. By January 2008, all applicable IRS functions incorporated procedures in their Internal Revenue Manual for the application and use of the indicator.

We are also building a comprehensive specialized reference source for our employees to understand quickly the appropriate treatment for taxpayers who call with identity theft issues. This reference will ensure that our employees follow the appropriate procedure to correct the taxpayer's problem and apply the indicator.

16. The recent revelation that State Department contract employees accessed the files of presidential candidates without authorization raises issues regarding the

vulnerability of personal taxpayer information. Describe the safeguards and procedures the IRS has in place to ensure that similar unauthorized access does not occur at the IRS. Describe the screening that is conducted on contract employees who will have access to confidential taxpayer and return information. Describe any training contract employees must complete before beginning work at the IRS and compare it to the training IRS employees receive. Provide examples of any certifications outside contractors must sign before beginning work at the IRS.

The IRS implemented the Unauthorized Access (UNAX) program in 1998 to safeguard against the unauthorized access of personal taxpayer information. Employees are only authorized access to taxpayer records when the information is necessary to carry out their tax administration duties.

The UNAX program includes comprehensive training and outreach to ensure all IRS employees and contractors understand and comply with UNAX policies, procedures and responsibilities. All IRS employees and contractors must complete briefings on Ethics, Information Protection, Privacy/Disclosure, Computer Security Awareness and UNAX during new employee orientation and annual mandatory briefings reinforce information protection policies. All employees are required to sign Form 11370, *Certification of Annual UNAX Awareness Briefing*, to document their completion of the UNAX briefing annually.

The IRS uses several systemic processes to track and flag a potential unauthorized access. Managers take an active role in preventing unauthorized access to taxpayer accounts by monitoring employees work assignments and consistently enforcing IRS' information protection requirements. Managers review weekly reports that flag suspicious accesses. Suspicious activities are identified by both the IRS and TIGTA.

TIGTA has responsibility for investigating unauthorized access incidents. Upon completion of the investigation by TIGTA, any suspicious activity that has been validated as an unauthorized access is adjudicated by the Workforce Relations Office of the IRS Human Capital Office with input from IRS management. Disciplinary actions include reprimand, letters of admonishment, suspension and termination.

IRS conducts the same background investigation for a contractor employee as it does for IRS employees. This background investigation includes a tax check and fingerprinting prior to being permitted to work for IRS. In addition, IRS includes confidentiality clauses in contracts requiring all contractors to protect all sensitive information. A letter of certification must be received from the Contracting Officer Technical Representative documenting the completion of the contractors background check before granting the contractor access to IRS systems and facilities. Form 11370, *Certification of Annual UNAX Awareness Briefing*, is completed and signed documenting completion of the annual UNAX mandatory briefing.

17. **Describe the training the IRS provides to employees on the policies for accessing taxpayer information. Describe how the IRS tracks and flags employee access to tax returns and return information. Describe how suspicious activity is investigated once it is flagged.**

The response to Question 16 above describes the process for training IRS employees and contractors on UNAX policies and procedures, systemic methods to flag potential unauthorized access and the process to investigate suspicious activity.

18. Describe how the IRS holds employees and contractors accountable for the security of taxpayer data. How many violations has the IRS detected during each of the prior three years? Describe any disciplinary actions and penalties the IRS has taken during the last three years for security violations.

Our three point plan for protecting sensitive information includes Prevention, Data Loss Management and Accountability. The IRS has taken additional action to ensure that employees and contractors are accountable for the protection of taxpayer information and other sensitive personally identifiable information (PII).

One of these actions is Operation R.E.D., a two-month enterprise-wide event from April to June 2008 focused on refreshing IRS employees' awareness of existing policies and procedures regarding the protection of Personally Identifiable Information (PII). During this event, managers held meetings with their employees to discuss the protection of PII, and employees will be asked to Review their possessions for PII, Encrypt or safeguard the PII they have a business need to keep, and Destroy or archive the PII they no longer need to keep.

The IRS is actively pursuing improved security for our information technology assets including:

- Implementing secure data transfer that resulted in eliminating tape exchanges with all external Trading Partners;
- Encrypting 100% of deployed laptops (52,500 units);
- Implementing protocols that require two lines of password defense to access the IRS network remotely (Two Factor Authentication);
- Initiating the implementation of encryption software to ensure that all removable media and desktops not located in IRS facilities are encrypted, and;
- Increased monitoring capabilities to detect IRS targeted phishing sites on the Internet, in order to enhance the protection of taxpayer information and other sensitive personally identifiable information (PII).

While we continue to experience the theft of laptop computers, encryption and other security improvements have dramatically reduced the associated loss of PII.

Laptop Losses	2006	2007	2008 (09/30/08)
Laptops Reported Lost	145	110	53
Laptops Recovered	17	34	14
Total Net Loss	128	76	39
Lost Machines Not Encrypted	26	06	3[1]

[1] None of the three unencrypted machines lost in 2008 had personal information.

During the prior three years, we initiated investigations for 1,468 possible unauthorized accesses. Although these cases represent only a small fraction of the millions of accesses each year by the IRS employees and contractors, the unauthorized accesses can damage the public confidence in the IRS.

UNAX	2005	2006	2007
Investigations Initiated	499	448	521
Completed Investigations Resulting in Disciplinary Actions	259	251	129

The decline in disciplinary actions from 2005 through 2007 is due to a number of investigations initiated that have not been completed and those cases where an unauthorized access was not substantiated during the investigation. Disciplinary actions for UNAX and other security violations include termination, suspension and letters of admonishment or reprimand and are determined by IRS management on a case–by-case basis.

19. **How does the IRS evaluate employee positions to ensure that employees have access only to the systems they need to carry out their job responsibilities? How often does the IRS reevaluate what systems employees need access to in order to carry out their job responsibilities?**

IRS evaluates employee system access needs on an on-going basis depending on the roles and responsibilities of the employee. The IRS requires management approval for system access requests for all employees and contractors. In addition, managers and employees are required to certify and document annually the continuing need for access to these systems.

20. **What steps is the IRS taking to evaluate its existing and future systems to identify potential weaknesses in the IRS's ability to detect and collect needed data, including transactions and audit trails, that can help determine whether IRS employees and contractors are illegally accessing taxpayer files?**

The IRS maintains strict technical and procedural controls over access systems that contain taxpayer data. These controls are reviewed and documented for all current and future system through the FISMA mandated Certification and Accreditation process. The primary system that is used to access taxpayer accounts is monitored by a sophisticated auditing system that detects when employees or contractors access accounts outside of the necessary scope to complete their jobs (e.g., If an employee accesses a neighbor's or relative's account, this will automatically be reported and investigated). This and other systems are routinely monitored for attempts to circumvent the security controls in place. These audit trails are monitored and analyzed by Cyber Security Specialists, who look for patterns of behavior over extended periods of time. The audit trails are also monitored by our Computer Security Incident Response Center, which monitors systems in real time for specific attacks or attempts to access data. The IRS is also developing additional capabilities for audit trail analysis that will increase its ability to correlate disparate events on different systems across the enterprise. The IRS has taken steps to prioritize this additional functionality to expedite deployment.

21. Please explain why the Identity Theft Summit planned for the summer of 2007 was cancelled. Are there plans to hold the summit in 2008?

In mid-2007, the IRS created PIPDS. The creation of this office included an evaluation of all existing programs and issues related to identity theft. We decided to postpone a previously scheduled summit in order to complete this evaluation and to stand-up the PIPDS office. We rescheduled the event as the IRS Identity Protection Forum, which was held in Washington, D.C., on July 21-22, 2008. The goal of the Identity Protection Forum was to unite key executives and experts in the fields of privacy and identity theft from both public and private sectors, in the domestic and international arenas, to share common experiences and successes in the protection of identity information and gain insights into trends and future developments in this area of growing interest.

The keynote address for the forum was delivered by Treasury Under Secretary Peter McCarthy. Douglas H. Shulman, Commissioner, Internal Revenue Service provided opening remarks and other key speakers included, the National Taxpayer Advocate, the co-founder of the Fraud Discovery Institute, the Director of the Homeland Security Council for Cyber Security and representatives from the Canadian Revenue Service, the FTC, Her Majesty's Revenue & Customs (United Kingdom), the Federal Bureau of Investigation, and the Government Accountability Office.

The IRS Identity Protection Forum has already proven successful in bringing together its participants to combat identity theft. For example, the IRS has held discussions with one of the Forum presenters to discuss vulnerabilities for identity theft in check cashing establishments and is now collaborating internally to identify possible opportunities for pursuing proactive identity theft solutions. In addition, the FTC Forum participants engaged PIPDS to collaborate with the FTC in developing an identity theft guide for pro bono attorneys. Also, one of the international participants, Her Majesty's Revenue & Customs from the United Kingdom, held a follow-up discussion on related issues with the Department of Justice.

22. Over the past few years, the IRS has created several identity theft program offices within various functions of the IRS. The most recent office is the Privacy, Information Protection, and Data Security (PIPDS) office. Describe the responsibilities of this office and all related offices, and how all the IRS identity theft offices and functions interact and interrelate.

To strengthen our enterprise-wide approach to identity theft and data security, IRS established the PIPDS office in July 2007. The PIPDS vision is to preserve and enhance public confidence by advocating for the protection and proper use of identity information. PIPDS does this by cultivating a culture where the protection of identity information is integrated into everyday business practices. In addition, the PIPDS office promotes comprehensive outreach and education programs for employees and the public to increase awareness and reduce vulnerabilities. The following three subordinate offices report to the Director, PIPDS:

- Office of Privacy
  - Promotes the protection of individual privacy and integrates privacy into business practices, behaviors, and technology solutions
- Identity Theft and Incident Management

- Identifies risks, reduces vulnerabilities for identity theft, and improves victim assistance
- Online Fraud Detection and Prevention
  - Reduces online fraud against the IRS and taxpayers

With the increasing focus on privacy issues, and the growing threat of identity theft evidenced by the dramatic increase in the detection of IRS-targeted phishing sites in 2007, the IRS has taken additional action to ensure that taxpayer information and other personal information are properly protected.

To what extent is any one office ultimately responsible for resolving cases of identity theft?

PIPDS is responsible for enterprise-wide oversight for the development and implementation of effective policies and procedures to resolve cases of identity theft effectively. PIPDS collaborates with business units across the IRS to develop and implement holistic solutions to assist the victims of identity theft.

The IRS opened a specialized identity theft victim assistance unit on October 1, 2008, dedicated to resolving tax issues incurred by identity theft victims.

How does the IRS know if an identity theft case has been resolved satisfactorily if one function does not have ultimate responsibility and accountability?

The IRS is applying several practices to ensure the satisfactory resolution of identity theft cases. Beginning in October 2008, the specialized unit will monitor identity theft cases of taxpayers through to resolution. The CSR will have the responsibility to monitor the taxpayer's cases to ensure the issues are resolved quickly and completely. In addition, the IRS will apply our quality review process to ensure that the taxpayers' issues were resolved satisfactorily. We use the results of the review process to improve our processes and procedures.

23. To what extent would the regulation of return preparers, including more thorough vetting of ERO applicants, affect the identity theft problem?

The IRS puts a high priority on maintaining taxpayer confidence in the e-file program. The Electronic Tax Administration (ETA) office within our Wage & Investment Division is currently re-evaluating the Electronic Return Originator's (ERO) application process to determine if changes could be made to strengthen the integrity of the IRS e-file program. The integrity of the ERO as our trusted partner is paramount to the success of the program.

We are currently evaluating the recommendations made by the ETA Advisory Committee in their 2008 Report to Congress. These recommendations include:

- accept only electronic ERO applications through e-services because of the additional identity validation done for e-services registration,
- perform criminal background checks and credit checks on 100% of ERO applicants, and
- increase monitoring of e-file providers.

We are already taking steps for next filing season to increase the verification process of applicants (principles or responsible officials of firms) to ensure they meet our suitability standards (e.g., verify citizenship claims, increase criminal history checks, etc.).

Questions from Senator Grassley:

1. **Most of the testimony this morning has focused on improving efforts to identify, track, and resolve cases of identity theft after they happen. While these efforts are critically important, it seems to me that with minimal effort, the IRS could help prevent identity theft before it happens.**

   As I noted in my opening statement, the IRS already uses a knowledge-based verification system to track refunds and permit electronic filing.

   If the IRS simply added a box to the printed tax forms – adjacent to the signature box – that allowed taxpayers to enter their previous year's AGI, it would go a long way toward preventing fraudulent tax returns.

   For those who lost last year's return, the IRS could simply hold their refund until April 15th to insure no one else files a return with the same name and social security number.

   Could you comment on this proposal?

   The IRS is building a strong prevention program to reduce proactively incidents of identity theft. This program is based upon three priorities: (1) reducing opportunities for thieves to obtain identity information, (2) reducing the opportunities for thieves to use the data they have stolen, and (3) increasing deterrence efforts to discourage identity theft.

   We are currently evaluating several proposals for enhancing e-file security and functionality. We are assessing the viability of these proposals using several factors including taxpayer burden, customer convenience and security. We will consider this recommendation in our evaluation. We continue to seek improvement to our processes to protect taxpayers and reduce the incidence of identity theft.

2. **In addition, as I noted in my opening statement, last year's immigration bill included a provision to allow workers to place a block their Social Security number – much like the FTC do not call list, or a credit freeze.**

   To prevent fraudulent tax returns, taxpayers could place a block on their SSN until they file their own return. An identity thief who tried to file a return before the taxpayer did would not be able to collect a refund because the SSN would be blocked, thereby alerting the IRS to the fraudulent return.

   Could you comment on this proposal?

   To achieve our goals for increasing the electronic filing of tax returns, we are concentrating our improvements on making e-file smarter to block the criminals more

effectively from committing electronic tax fraud. This includes evaluating additional enhancements to e-file security and functionality. Given the benefits of electronic filing, and the volume of account-related contacts that would be needed to block and unblock filings each year, we believe this proposal would be more burdensome for taxpayers than the development of IRS filters that will accomplish the same effect.
As part of our updated Identity Protection Strategy, we are developing proactive initiatives to enable identity theft victims to reduce future harm. This includes evaluating additional enhancements to e-file security and functionality. We believe that we can provide the best taxpayer service by focusing on preventing perpetrators from filing fraudulent returns.

We use the identity theft indicator to mark the taxpayer's account and to prevent victims from encountering the same problems year after year. We will use this indicator in our screening process and compare the characteristics of the filed return with the historical filing characteristics of the taxpayer. Our employees will review suspicious accounts and interact with the taxpayer to verify that the taxpayer, and not the perpetrator, submitted a legitimate return.

Questions from Senator Snowe:

1. **One method of online identity theft, phishing, seems to be spiraling out of control. More than 3.5 million Americans lost money to phishing schemes and online identity theft over a 12 month period ending in August 2007—this is a 57 percent increase over the previous year. And the total amount lost by the victims, $3.2 billion dollars.**

   Over the past 6 months the IRS has issued six separate warnings on phishing scams related to the IRS, and has significant information on suspicious emails and identity theft—including what steps taxpayers can take to protect themselves.

   While consumer awareness is critical in fighting against identity theft and phishing scams, can't there be more done legislatively to provide greater enforcement and stiffer penalties to act as a deterrent to curtail criminals from engaging in these fraud activities? If we just focus on awareness that might not that might not reduce the prevalence of phishing scams, right?

   In addition to our outreach efforts on phishing, the IRS has established the Office of Online Fraud Detection and Prevention (OFDP) within the Office of Privacy, Information Protection and Data Security (PIPDS) to address the increasing and evolving threat of online fraud affecting the IRS and taxpayers. The mission of this office includes:

   - A rapid response capability to detect and mitigate against online fraud incidents;
   - A robust analytic and operational information sharing capability to prevent and reduce risk;
   - Use of technological innovations and process improvements to tackle current and next generation online fraud schemes; and

- Comprehensive online fraud awareness, training and education programs with public and private sectors to reduce vulnerabilities and minimize the severity of online fraud.

OFDP is working closely with the IRS Criminal Investigation (CI) Division, the Treasury Inspector General for Tax Administration, the Department of Justice, the Federal Bureau of Investigation and the Federal Trade Commission (FTC) to pursue criminal investigations as appropriate. We will work with the Department of Treasury on proposals for legislative change related to enforcement and penalties that are identified and determined to be appropriate.

2. **In 1998, Congress established a goal for the IRS that, by 2007, 80 percent of all returns be filed electronically. However, approximately 58 percent of individual taxpayers filed electronically last year. The IRS said it expects to reach the 80 percent milestone by 2012.**

   If phishing and other online tax scams continue to persist, will it hamper our ability to reach the goal we set 10 years ago?

   Any breach to the public confidence that e-file is safe and secure will hamper the ability to reach the 80% goal. We are taking several actions to ***preserve*** and enhance public confidence and address the increasing and evolving threat of online fraud as discussed in the response to Question 1.

   The IRS puts a high priority on maintaining taxpayer confidence in the e-file program through its certification of individuals who submit electronic returns called Electronic Return Originators (EROs). The Electronic Tax Administration (ETA) office within our Wage & Investment Division is currently re-evaluating the (ERO) application process to determine if changes could be made to strengthen the integrity of the IRS e-file program.

   The integrity of the ERO as our trusted partner is paramount to success of the program. We are currently evaluating several proposals made by the ETA Advisory Committee in their 2008 Report to Congress. These recommendations include:

   - Accept only electronic ERO applications through e-services because of the additional identity validation done for e-services registration;
   - Perform criminal background checks and credit checks on 100% of ERO applicants; and
   - Increase monitoring of e-file providers.

   We are already taking steps for next filing season to strengthen the verification process for applicants (principles or responsible officials of firms) to ensure they meet our suitability standards including verification of citizenship claims and criminal history checks.

3. **Since August 2007, the IRS has issued six separate warnings on phishing scams related to the IRS. In addition, the IRS recently reported that, for 2007, it found approximately 900 phishing web sites that exploited the agency. 2008 looks to easily eclipse that figure significantly—as of March 19, the IRS has already found**

close to 730 phishing sites that attempt to trick taxpayers into providing personal information.

a. Can the IRS elaborate on how it deals with the IRS-related phishing sites from discovery to take down?

The IRS has established the OFDP office within PIPDS to address the increasing and evolving threat of online fraud affecting the IRS and taxpayers. One of the functions of this office is to maintain a rapid response capability to detect and mitigate against online fraud incidents. OFDP has developed a team of highly trained security specialists to detect suspicious websites, analyze their content, and ensure that these sites are shut down. Since October 2007, this unit has identified and shut down approximately 2,500 fraudulent sites from all over the world. OFDP has also developed a rapid response capability. For October 2007 through July 2008 the median time for fraudulent site detection to site shut down within the U.S is 3.5 hours. The IRS Criminal Investigation (CI) Division and the OFDP office are working closely with the Treasury Inspector General for Tax Administration (TIGTA), the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI) and the Federal Trade Commission (FTC) to identify perpetrators and pursue criminal investigations as appropriate.

b. Has the IRS ever been hindered in getting a phishing site removed or shut down?

Sometimes the IRS experiences problems in getting a phishing site removed or shut down because many of the phishing sites originate from overseas. These international sites can be more challenging to deal with than domestic sites due to the different legal and political realities in certain countries. For October 2007 through July 2008, OFDP's rapid response capability internationally has a median time for fraudulent site detection to site shut down of 10.4 hours. International sites are going be to a continuing challenge to the IRS, even with stronger legislation, due to social and political challenges intrinsic to certain countries.

c. Has the IRS received any complaints about misleading or deceptive domains or websites that unduly confuse taxpayers due to the lack of such site not clearly detailing it is not associated with the IRS?

Yes. There were a few instances where we have requested that site owners clarify/modify their domain names or content hosted on their website, and they have complied.

Questions from Senator Smith:

1. **Credit monitoring seems to have become the de facto service offering to people who are part of a data breach population. But, the service really doesn't do anything for somebody who falls victim to identity theft; it will only tell them that they have a problem. From that point on, they are on their own and will likely spend 40 to 60 hours cleaning up a mess that they didn't create. Wouldn't it be more meaningful to citizens if we were to offer them victim recovery assistance**

instead? In other words, rather than simply tell somebody they have a problem, actually help them solve it?

The IRS includes victim recovery assistance as part of the service offered in the notice sent to taxpayers who are at high risk of harm following a data breach. Using the GSA contract, the IRS is providing 3-in-1 credit report and credit monitoring services for one year to all notified taxpayers including unlimited access to the report and alerts that may be a warning of identity theft. This service also includes $20,000 identity theft insurance, and premium Customer Care with a dedicated 1-800 hotline available for personalized identity theft victim assistance.

The IRS has determined that by providing credit monitoring services to our taxpayer coupled with 24/7 customer assistance and cost reduction insurance, we are providing an effective way to mitigate the risk and may assist taxpayers in early detection of identity theft. We are continuing to evaluate the credit monitoring and victim recovery assistance options available and are working closely with the General Services Administration to ensure that as additional options become available, the IRS continues to proactively evaluate those options and procures those services that provide the greatest benefit to taxpayers who are at high risk of harm following an IRS loss of personal information.

On October 1, 2008, the IRS opened a specialized unit dedicated to resolving tax issues incurred by identity theft victims. This unit will enable victims to have their questions answered and issues resolved quickly and effectively. Victim assistors will handle taxpayer inquiries from multiple sources including a dedicated identity theft telephone line. We will ensure that identity theft issues are resolved by preparing our employees with the expertise to address each issue. Our goal is to resolve issues promptly and permanently.

Questions from Senator Schumer:

1. **Commissioner Shulman, I know this is not the focus of the hearing, but I would like to address the issue of electronic filing. I am very supportive of the free file program for taxpayers making less than $55,000 a year. But that program doesn't go far enough – I think the issue of free tax PREPARATION should be considered separately from the issue of free electronic FILING. I think that people shouldn't be charged to file their taxes electronically when it actually saves the government money to process an e-filed return.**

   Yet the current situation is that people who do not qualify for the free tax preparation and end up buying one of the popular tax programs like Turbo Tax, or going to H&R Block or Jackson-Hewitt, are charged an additional filing fee, on top of whatever it costs to buy the tax filing program or preparer service. I think this is unfair. I'm sure in this age of technology it's a very simple matter for companies to transmit tax returns electronically to the IRS. Since boosting the rate of e-filing is a priority for the IRS, and electronically filed returns are less expensive to process, why should people be charged for the privilege? It seems

to me that it's backwards – you should get to e-file for free, and be charged for a paper return. But we do it the opposite way. Why?

The IRS maintains agreements with IRS-Authorized E-File providers who build and maintain the e-filing infrastructure. The IRS also imposes specific security and transmission requirements to ensure taxpayer data is protected. These requirements involve costs that are currently borne by third parties. Additional infrastructure costs would be required in the IRS were to take in these returns directly.

The fees that taxpayers incur are levied by IRS-Authorized E-File providers who support third-party systems that the IRS relies on to deliver 60% of individual tax returns electronically filed in 2008. There are indications that market pressures are driving out e-file charges. For example, during this past filing season, commercial products were available to some taxpayers that offered both free tax preparation and free tax filing. In addition, IRS Free File is available to approximately 70% of the taxpayers. Early indications for the coming season suggest that more companies may be moving away from e-file charges.

Despite this trend, a charge for e-filing is one of a number of barriers that may inhibit growth in e-filing. The IRS is conducting a comprehensive study to identify opportunities to advance electronic filing. Our objective is to meet the Congressional goal that 80% of returns be filed electronically. The first part of the study will analyze taxpayer and tax professional behavior, review the role of state and local governments in tax administration and discuss the various options to be considered for advancing e-filing. These options will include: incentives, mandates, direct electronic filing, telephone-based filing and bar-coding.

The second part of the study will involve analysis of key findings and an assessment of various options. This study will not make recommendations; it will only generate different scenarios based on various options to determine the benefits, costs and the possible increase in electronic filing. In addition, the study will specifically estimate the effect that electronic filing fees have on the e-filing rate and will examine ways to address this problem.

2. **If legislation were passed that required the IRS to develop a free online portal where forms could be filled in by taxpayers and electronically – not tax prep software, but fillable PDF forms that could be filled out by taxpayers and submitted online – how long it would take for the IRS to develop this portal?**

   The IRS is currently conducting a study of potential options for advancing the use of electronic filing. Part of that effort will involve an analysis of the technical and infrastructure requirements needed to support the system you describe. We will have more information available to respond to your proposal when the study is completed in the Spring of 2009.

3. **I sent a letter to Mr. Shulman and Ms. Stiff on March 6 asking why we were wasting $42 million of taxpayer money to send notices to people about the stimulus checks, when there was plenty of news coverage about the stimulus plan and the taxpayers receiving the notice would be receiving the checks**

automatically. I haven't received a response to that letter. Wouldn't that money have been better directed at enforcement efforts?

The IRS has responded to these concerns in a letter dated April 15, 2008, a copy of which is attached as Appendix A.

4. **There is a story in today's *New York Times* about how a certified tax preparer on Long Island was charged with filing false tax returns using the names of former clients to try to collect at least $19 million in fraudulent refunds. The story says that the IRS did nothing about the case, and that the fraud was discovered by local authorities. My question about this situation is this: Presumably, if the returns are being filed using the names of former clients, it would mean that two returns were being filed for the same taxpayer, with the same Social Security number. Why wouldn't the IRS systems catch this automatically?**

   The IRS uses a variety of automated systems and techniques actively to detect filing fraud and catch identity theft. The IRS' CI Division uses the Electronic Fraud Detection System (EFDS) to screen questionable returns and continues to improve ways to identify and analyze fraudulent tax refund schemes involving identity theft. We have developed new filters to identify new crimes as the techniques used by identity theft criminals evolve. For example, we recently developed a filter to identity those returns that have been stolen by a perpetrator through a phishing scheme.

   The Fraud Detection Centers (FDCs) within our CI Division continue to improve ways to identify and analyze fraudulent tax refund schemes involving identity theft. The FDCs forward those returns meeting the appropriate criteria to our field investigation offices to develop potential recommendations for prosecution.

   We use the identity theft indicator to mark the taxpayer's account and to prevent victims from encountering the same problems year after year. We will use this indicator in our screening process and compare the characteristics of the filed return with the historical filing characteristics of the taxpayer. Our employees will review suspicious accounts and interact with the taxpayer to verify that a legitimate return was submitted by the taxpayer and not the perpetrator.

   a. **Commissioner Shulman, I want to know what the IRS plans to do to protect the millions of taxpayers whose personal information you are holding in your databases. Another disturbing recent report from the Inspector General details serious gaps in the security of IRS computer networks. Will you take steps to protect the IRS's vulnerable computer networks? Can you commit to a date when the problems in this report will be fixed?**

      The IRS is taking several actions enhance the security of the IRS computer networks. First, the IRS is implementing an enterprise-wide risk management system that focuses resources on major systems and assets that support the most critical business processes supporting tax administration. We are ensuring that proper management, operational and technical security and privacy controls are enhanced for existing legacy infrastructure systems, and we are building these controls into the designs for all new tax modernization systems. These activities support enhanced protection of taxpayers' personal information.

The IRS continuously monitors the day-to-day security status of the entire IRS network, all applications, databases and computer operations by a world-class 24x7 Computer Security Incident Response Center (CSIRC). The IRS CSIRC provides proactive prevention, detection and response to computer security incidents targeting the IRS' enterprise information technology (IT) assets. The CSIRC is equipped to identify, contain and eradicate cyber threats targeting IRS computing assets. The four major CSIRC operational functions of prevention, detection, response and reporting meet Federal Information Security Management Act requirements for incident response and reporting. IRS IT security technical efforts have focused on "hardening" computer and network infrastructure systems to make them resistant to external attacks. There have been no successful penetrations into any IRS systems by hackers. The IRS has deployed the security "defense-in-depth" approach with over 100 firewalls and several hundred intrusion detection devices, with all of these devices monitored by the CSIRC. Anti-virus software is deployed throughout the network, and the latest security patches and required updates are aggressively pushed out to all desktops.

b. **The IRS reports that it does not alert employers when they have an employee with a complete case of identity theft because they are not allowed to disclose that tax information. However, there are several exclusions in the IRS code that do allow this disclosure to ensure proper law enforcement. Have you examined whether the IRS is taking full advantage of the tools available to you under existing law? What other authorities could Congress give you to enable the IRS to share limited and necessary information with employers if they find a case of suspected identity theft?**

As part of our Identity Protection Strategy, we are currently reviewing the disclosures we are permitted to make under current law in identity theft cases to employers and to non-tax administration law enforcement. When this review is complete in late Fall 2008, the IRS will evaluate any proposals for additional disclosures for legal, procedural and technological implementation. We will work with the Department of Treasury on recommended proposals for legislative change if any are identified and determined to be appropriate.

Appendix A

COMMISSIONER

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

April 15, 2008

The Honorable Charles E. Schumer
United States Senator
Washington, DC 20510

Dear Senator Schumer:

This letter responds to your inquiry of March 6, 2008, expressing concerns about the way the IRS notified individuals about payments they may receive as a result of the Economic Stimulus Act of 2008.

As you know, we mailed the first notice to 133 million taxpayers who filed a tax return in 2006. We also mailed a specially designed notice to approximately 20 million Social Security, Railroad Retirement, and Veterans Affairs beneficiaries, who may be eligible for a stimulus payment and might not normally need to file a return.

Leadership of a large and complex organization, like the IRS, requires constant judgment calls about how to best allocate resources based on the information available

Our decision to send the notice was influenced by our experience delivering tax rebates in 2001, when the magnitude of calls from citizens seeking information overwhelmed our phone system and temporarily shut it down Importantly, the 2001 rebates occurrec in the summer - *after* the peak service demands of filing season were over.

To avoid repeating this experience, we decided to proactively send notices to the 133 million taxpayers informing them of their potential eligibility to receive a stimulus payment and telling them that they did not need to take action beyond filing a 2007 tax return in order to receive their stimulus payment. By doing so, we believe that we averted millions of calls and potential disruptions at the peak of the normal filing season

As with all decisions, we are monitoring whether we achieved the results that we wanted out of this program and will make future adjustments based on what we learn.

I hope this explanation of our decision is responsive to your concerns. I take questions about the use of taxpayer funds very seriously. If you would like to discuss further, or need more information, please call me or contact Floyd Williams, Director, Office of Legislative Affairs, at (202) 622-3270.

Sincerely,

Douglas H. Shulman

Senator Schumer -

As you know, I'm 3 weeks into the job. I'm looking forward to working together.

Identity theft: Who's got your number?
U.S. SENATE COMMITTEE ON FINANCE
U.S. Senator Olympia J. Snowe
April 10, 2008

Mr. Chairman, thank you for your tremendous leadership and stalwart commitment on matters affecting taxpayers and taxation in this country. Like my colleagues on the committee, I am immensely grateful to you for holding this hearing to examine the effect of tax related identity theft on victims and how the IRS can improve its identity theft strategy. I appreciate the testimony of our witnesses today, especially Commissioner Shulman who is making his first appearance before this Committee as Commissioner of the IRS.

It is agonizing enough for taxpayers to have to perform this annual ritual of filing tax returns—compiling countless numbers, looking for old receipts, and deciphering through pages and pages of tax code. But the difficulty that taxpayers go through during tax season is compounded by a very real and growing problem of identity theft.

Recently in Maine, Hannaford Brothers, a regional chain of grocery stores announced that there had been an intrusion into their computer system. This breach resulted in 4.2 million customers whose debit and or credit card numbers were compromised, already more than 1,800 victims have reported fraudulent activity on their accounts.

Computer networks are increasingly susceptible to hackers, intruders and other cyber criminals, all of which try to steal your personal information. Unfortunately, these attacks are becoming more frequent and more severe, and the perpetrators are becoming harder to identify and bring to justice.

One of the ways in which these intruders to try to steal your information is Phishing, a method of online identity theft that takes the form of fraudulent e-mails or websites to deceive the recipient into giving personal or financial information. In general, identity theft is the number one consumer complaint in the United States, far outpacing all others. The Federal Trade Commission reported that identity thefts related to tax refund fraud increased *396 percent* from 2002 to 2006. Identity theft has gotten so bad that the IRS National Taxpayer Advocate Nina Olson reported to Congress earlier this year that identity theft is one of the "most serious problems" facing taxpayers.

While the majority of identity theft is paper based—stealing credit cards, account statements, or receipts—online identity theft is increasing, in part due to phishing scams. Since August 2007, the IRS has issued six separate warnings on phishing scams related to the IRS. In addition, the IRS recently reported that, for 2007, it found approximately 900 phishing web sites that exploited the agency. 2008 looks to eclipse that figure significantly—as of March 19, the IRS has already found close to 730 phishing sites that attempt to trick taxpayers into providing personal information.

Typically, these scams or sites, revolve around a refund-related bogus e-mail, which falsely claims to come from the IRS, telling the recipient that they are eligible for a tax refund, and instructs the recipient to click on the included link to access a refund claim form. These scams aren't just targeting individual taxpayers, one version of the refund scam appears to be directed toward tax-exempt organizations that distribute funds to other organizations or individuals.

To combat this problem that is spiraling out of control, I along with Senators Nelson and Stevens introduced the Anti-Phishing Consumer Protection Act of 2008 earlier this year. This critical legislation would explicitly prohibit the practice of phishing—the deceptive solicitation of a consumer's personal information through the use of emails, instant messages, and misleading websites that trick recipients into divulging their information to identity thieves. It would also prohibit related abuses, such as the practice of using fraudulent or misleading domain names of government agencies, nonprofit organization, and companies, by defining them as deceptive practices under the FTC Act.

In 1998, Congress established a goal for the IRS that, by 2007, 80 percent of all returns be filed electronically. While we felt short of reaching this goal, more taxpayers are embracing the Internet to file their returns. However, online identity theft and phishing are hindering our ability to achieve these goals because these scams erode consumer confidence in feeling secure when using the Internet for these activities since phishing and other online fraud activities directly undermine the vital trust and security that is a requisite.

In sum, Mr. Chairman, although Congress has a duty to write the tax code, we also have an obligation to ensure that it is administered properly being cognizant of the fact that taxpayer's privacy rights should not be compromised by the collection of revenue. Thank you, Mr. Chairman.

Identity Theft: Who's Got Your Number?
Hearing Before the Senate Finance Committee
Statement of Rebecca Spencer
April 10, 2008

Thank you, Chairman Baucus and Ranking Member Grassley, for this opportunity to share my experience regarding tax related identity theft with the members of the Senate Finance Committee.

In 1975, I took over a home based tax practice with about 1600 clients from my uncle. Since that time the business has grown to over 6500 tax clients annually. As an Enrolled Agent, I have always been a strong supporter of e-file; in fact, my office was the first e-filer in the State of Montana.

At first, e-filing was very restricted, with identity checks and compliance visits to all Electronic Return Originators (EROs). I felt quite secure that my client data was not something an identity thief could use. Since that time, e-filing has been opened up to the entire world. Anyone with a little prior planning can take a laptop into a cyber café with a stolen identity, including a valid employer identification number, and file a United States income tax return.

On January 14th of this past year, three days after e-file opened, one of my long time clients came to the office and filed her tax return. She usually filed in February but this year she was in desperate need of the money. The following morning, instead of a refund loan check, we got an IRS acknowledgement that her return had already been filed. Someone had used this single, financially struggling mother of two's identity and filed a tax return on January 13, well before most people get around to filing.

My client was in tears and I realized we had a real case of identity theft on our hands. Not knowing who to call in the IRS, I started with the Criminal Investigation 800 number. The recording there states, "If you would like to file Form 3949A [an Information Referral to report tax fraud] please order this form by calling 1-800-IRS-FORM. This form can also be ordered on our web site at www.irs.gov". There was not even an option to leave a name and phone number or wait for a representative.

I called the IRS e-help desk at the Service Center and their response was: "She will have to mail in a paper return."

Next, I sent my client down to the local IRS walk-in center, where she was told to file a paper return. As an Enrolled Agent, I felt that because the taxpayer's name and social security number were on the return she should have been entitled to a transcript - but the IRS refused. *She was denied access to her own tax account.* The walk-in office could not help until she gave them a social security card, driver's license, birth certificates, a letter of explanation and a written copy of the police report (which took

several days to get). After that, she was referred to yet another IRS function, the Taxpayer Advocate Service, which eventually was able to resolve her case.

The taxpayer was worried that her children's identities had also been stolen, but the IRS could tell her nothing until after she waited for the police report. I called the refund loan bank and was able to find out that the thief had filed as single without dependents, worked for a major US employer, had filed on-line, and applied for a refund loan credit card (a stored value card) instead of a check. (It is my understanding that with the stored value card the thief can go to an ATM with the password, thus avoiding the need for fingerprints or picture identification.)

The bank had not given the loan because the withholding was too high on the W-2. After my call to the bank, the return was flagged and when the tax refund arrived at the bank the money was held until the IRS was able to decide which taxpayer was legitimate.

Bottom line: *Ten days after the Internal Revenue Service had been notified that there was a problem, the Service released a refund to the fraudulent taxpayer.* It was only because I called the bank and gave them a heads-up about the identity theft that the refund was held up and not issued to the fraudulent taxpayer – *not because of anything the IRS had done to stop it.* Two months later, after contact with at least four IRS functions, the victim, with the help of the Taxpayer Advocate's Office, finally received her tax refund.

My office gets calls early in the tax season asking to prepare the return from a final pay stub. When we tell them we are unable to do so they say, "I'll just do it myself on the internet." (Another entire subject is how easy it is to print anyone's W-2 off the internet.) A taxpayer who is not following the rules only needs last year's employer identification number to file early. Among these early filers are the thieves filing a return with a stolen identity.

These returns are a financial drain on the system because they result in audits, amended returns which must be filed, or, as would have been the case had the bank not held the fraudulent deposit, outright loss of the refund amount.

My client had her identity stolen as a result of the theft of a government credit card. Another client had his wallet stolen. Identity theft can happen to anybody under the most normal of life's circumstances.

Several possible safeguards come to my mind:

1) Require the W-2s to be turned into Treasury electronically prior to being given to employees instead of one month later.

2) Do not open e-file to the general public on the internet until the W-2s are required to be in the taxpayer hands.

3) Annually give each employer a two letter code that must be included on the W-2 and require the code be entered on the e-filed return. This would prevent thieves from using prior year W-2 information to file fraudulent returns.

4) Have the taxpayers not using paid preparers fax their W-2 to the IRS or have them scan it into the software. Back in the days when we filed paper, everyone waited until they received a W-2 that they attached to the return. The dishonest weren't so prone to add an extra digit to the IRS withholding.

5) Have available a special mail stop for Electronic Return Originators or better yet have a way for irregular returns to actually go through electronically and *automatically stop the refund* on the previously used Social Security number until the legitimate filer can be identified. At present it is my understanding that Financial Management Service has NO way to stop the transfer of funds.

6) Require on-line filers to enter the prior year adjusted gross income or hold the processing until AFTER the 8453 [the signature form] with W-2s attached has been received by the Service.

I am sure many if not all the above suggestions can be met with excuses as to why they cannot be implemented. I would like to remind you of the year Senator Baucus suggested social security numbers of dependents had to be entered on the tax forms. Did the IRS do anything with the social security numbers for the next ten or so years? No—but how many dependents disappeared because the SSNs had to be reported?

The do it yourself software a presents a finished product that is difficult for the untrained eye to distinguish from a professionally prepared tax return. If the IRS issued bold easy to read warnings about preparers who do not sign returns, taxpayers who file prior to getting their W-2, and stealing identities or dependents (along with some big dollar fines connected with the practices) perhaps we would at least have taken one step in discouraging identity theft and the financial drain that results.

I believe the proposed tax practitioner registration and accompanying requirements will also help to eliminate incompetent return preparers who may be more prone to fraudulent practices.

Thank you again for this opportunity to testify and share my experience and ideas with a committee that has acted so diligently to preserve the integrity of the tax system over the years.

Responses From Rebecca Spencer to Questions for the Record
April 10, 2008 Hearing on Identity Theft

Question From Chairman Baucus

During the hearing, you provided several recommendations for the IRS to improve its identity theft strategy and indicated you had additional suggestions for ways the IRS could more effectively deal with identity theft. Please submit a complete list of your recommendations for the record.

In answer to your request for the suggestions how the IRS could effectively deal with identity theft, the first line of defense would be to prevent it from happening in the first place. In the last couple of years in the effort to make online e-filing easier the security items such as a PIN number that used to be mailed out to Tele-file prospects has been eliminated along with the 8453 and a last years adjusted gross income figure.

(1) Require the W-2s to be turned into Treasury electronically prior to being given to employees instead of one month later. Do not open E-file to the general public on the internet until the W-2s are required to be in the taxpayer hands.

(2) Annually give each employer a two-letter code that must be included on the W-2 and require the code be entered on the E-filed return. If the IRS cannot program this into their computers, make the software companies do it and not allow the return to be transmitted until the code is in place.

(3) Require online filers to enter prior year adjusted gross income OR hold the processing until an 8453 with W2s attached has been received by the service center. At present the preparer PIN system can be used on self-prepared returns, thus opening the floodgates for fraud.

(4) Have online filers fax copies of W-2s to a dead-end number at the IRS. Remember when you suggested all the children needed SS numbers? Nothing was done with them for ten years but the kids disappeared.

(5) I also personally believe that if the free file alliance was not allowed the bait and switch to refund anticipation loans, that those who want loans would go to legitimate preparers who are required to get picture ID and Social Security card copies from new clients, thus eliminating the anonymity of the internet. Stepping up the legislation on preparer registration with responsibilities and privileges would help weed out the Earned Income fraud perpetrators in addition to reducing identity theft.

After the identity theft has happened :

There could be a special mail stop for Electronic Return Originators—or better yet, actually allow irregular returns to go electronically so the service does not have to hand process them. Give us instructions what documentation to attach to prove our client's identity.

Since the Treasury can stop refunds for child support, why can't they be stopped in a similar way for identity theft if it is discovered before the refund has been released? Under the present system the refund loan banks are actually returning to Treasury millions of dollars in fraudulent refunds.

The list of original recommendations was in my written testimony.

Questions From Senator Snowe

> **One method of online identity theft, phishing, seems to be spiraling out of control. More than 3.5 million Americans lost money to phishing schemes and online identity theft over a 12-month period ending in August 2007—this is a 57 percent increase over the previous year. And the total amount lost by the victims, $3.2 billion dollars. Over the past 6 months the IRS has issued six separate warnings on phishing scams related to the IRS, and has significant information on suspicious emails and identity theft—including what steps taxpayers can take to protect themselves.**
>
> **While consumer awareness is critical in fighting against identity theft and phishing scams, can't there be more done legislatively to provide greater enforcement and stiffer penalties to act as a deterrent to curtail criminals from engaging in these fraud activities? If we just focus on awareness, that might not reduce the prevalence of phishing scams, right?**

Penalties for phishing schemes sounds like great legislation. Because so many of them take place overseas perhaps written into the legislation could be provision for the perpetrators to be arrested and charged if they enter U.S. soil. This COULD make some foreign criminal slow down a bit. One of my great fears is that someone could get through my firewall and steal the identities of my clients. This thief could be a foreign terrorist and phony returns could be e-filed from Iran and into bank accounts where funds were out of the country before most of my clients filed.

We ask our clients to contact us prior to responding to any IRS notice. They of course contact me with these phishing e-mails. When you go to the site even I cannot tell it is not legitimate because the Treasury logo and everything is there. This type of impersonation of the federal government is a problem in many areas, be it identity theft schemes or just marketing schemes that threaten problems if someone doesn't hand their posters or etc. I was wanted to know some information on a well-known TV evangelist about a year ago and what looked like his legitimate site had an offer for "pictures of our

Sunday school teachers." I managed to find the correct site and e-mail them about the clone. It is a problem in EVERY area. I even looked up my own site at about the same time and found where scammers were trying to grab clients into their sites for tax preparation.

You are right that more public education of not responding to IRS e-mails or phone calls is critical.

In 1998, Congress established a goal for the IRS that, by 2007, 80 percent of all returns be filed electronically. However, approximately 58 percent of individual taxpayers filed electronically last year. The IRS said it expects to reach the 80 percent milestone by 2012.

If phishing and other online tax scams continue to persist, will it hamper our ability to reach the goal we set 10 years ago?

In my opinion at the present the IRS has thrown all caution to the wind by not requiring at the minimum last year's AGI on all self-filed returns in an effort to meet the E-file goal. This present system where anyone could file my tax return from anywhere in the world as long as they had my Social Security number, first four letters of my last name, and any legitimate employer ID number puts not only potential identity theft individuals at risk but also the financial security of our nation.

If the IRS is so overworked with processing, putting their resources into e-filing of amended returns would help (of course there would not be as many of them if the free on line E-file was not used by early taxpayers who do returns off final pay stubs.) Also, if there was a free place to file W-2s themselves by employers. Most of the software companies who prepare 941s and W2s for small businesses do not offer free E-filing of these documents or even E-filing at all. The alternative is to go to the Social Security web site and E-file them there BUT all the data must be again hand keyed in. This is true with the 941s as well. Stamps are a great deal cheaper than the time involved to re-input and thus e-file these documents.

I have had GREAT success with e-filing corporate returns but the fiduciary has not been so successful. It is hard to decide WHAT name the system wants. With the 1041 I always have the clients sign a copy for me to mail in case the e-file fails. The e-file fails about half the time so the 1041 gets mailed. Most accountants are not e-filing corporate and partnership returns in my state because the Montana return must go paper. Requiring paid for computer prepared returns to be e-filed would be an option and is one that many states enforce.

COMMUNICATION

From the desk of Keisha [redacted]
Tel: 212-[redacted]
April 15, 2008

U.S. Senate Committee on Finance
219 Dirksen Senate Office Building
Washington, DC 20510-6200
(202) 224-4515

Subject: Identity Theft Victim's (Redacted) Comment Regarding the U.S. Senate Committee on Finance Hearing April 10, 2008 - "Identity Theft: Who's Got Your Number?"

Dear Chairman Baucus, Ranking Member Grassley and Members of the Committee:

My name is Keisha [redacted] and I am writing in response to the above referenced hearing on identity theft. It is noteworthy to say, I submitted written testimony to the NY State Consumer Protection Board this year as well. I am a native New Yorker and an advocate of quality public education for all. I graduated from the NYC public school system and went on to earn an undergraduate degree in Marketing vis-à-vis the Higher Education Opportunity Program (HEOP). In 1969, legislation established the Higher Education Opportunity Program (HEOP) at independent colleges and universities in New York State, to provide access to higher education for "educationally and economically disadvantaged" students. As a direct result, I was inspired to continue my education earning an MBA in Finance, with distinction, while working full-time on Wall Street. Moreover, it was God's grace that delivered me from the World Trade Center disaster unscathed on September 11th, so that I can do what I enjoy most -- educating the public.

THE PROBLEM

Identity theft in all forms, criminal, financial and medical, are symptoms of a problem. The problem is the unnecessary, unauthorized and/or illegal collection, sharing, unfettered access to, use and abuse of personal information. In my personal experience, identity thieves filed a fraudulent tax return and cashed a refund check of more than $5,000 through the IRS, H&R Block and HSBC Bank; obtained ID from the Department of Motor Vehicles (DMV) in Pennsylvania; secured employment; healthcare; cell phones; housing; and opened at least one Commerce Bank account to deposit counterfeit checks.

OFFICE OF THE COMPTROLLER OF THE CURRENCY (OCC)

As I prepared to file my taxes in 2005, I called the IRS to discover that a fraudulent, electronic tax return was filed and a refund was issued for more than $5,000 using my name, social security number, a fraudulent address, DMV issued identification and W2. For the first time in my life I found myself in a police precinct, in two states. Shortly thereafter, my money was stolen from my business account at the hands of Commerce Bank employees and identity thieves. I did not maintain any personal accounts with Commerce Bank; it is my contention that Commerce Bank employees knowingly facilitated the theft from my business account where I was listed as the authorized signor. News reports in May 2005 revealed that former employees of Commerce Bank, Bank of America and other financial institutions, were arrested in connection with a massive bank data theft scheme affecting over 500,000 accounts. I immediately sought legal counsel, to no avail. Attorney after attorney said "good luck". Either there was a conflict of interest; legal fees were beyond my means; or attorneys did not want to risk losing future clients, national banks guilty of negligence and violating its own privacy policies.

Commerce Bank confirmed that I was a victim of identity theft in its response to my written complaint to the Office of the Comptroller of the Currency (OCC). The OCC proved to be useless when it comes to consumer complaints; there is a conflict of interest as it pertains to the OCC's dual role as regulator and the authority that approves bank expansion plans, as it did with Commerce Bank after the massive bank data theft scheme was disclosed in the news. To make matters worse, when I followed up on my written OCC complaint, after months of inaction, I was told the individual to whom my complaint was addressed to at the OCC does not exist. It was/is an "alias". That is unacceptable and intolerable. Ironically, the OCC is funded through bank contributions instead of the appropriations process, thus it should be absorbed by or combined with a regulator that enforces the law and exercises prudent, proactive supervision. As a direct result of Commerce Bank's negligence, I was emotionally and financially distressed for almost two years, I lost all of my assets and I am no longer creditworthy, as my credit scores went from 700+ before the fraud at Commerce Bank to unspeakable scores today. Criminal justice officials (DOJ) acknowledge that victims of financial crimes, such as bank fraud, identity theft, and elder financial exploitation, may suffer severe psychological and financial harm and physical effects as well.

IRS

In my dealings with the IRS, I was troubled to learn several things. First, the IRS did not and does not have a mechanism for dealing with fraud. I was given a toll free number to call to report the identity theft in 2005, however, there was no reference or tracking number, correspondence or follow up. I was told my complaint would be forwarded to the Criminal Investigation Division, but I would not receive any response or update regarding the complaint. The only information I have is the agent's information when I called to report the fraud. The IRS did nothing with the information provided.

Second, I learned coincidentally that the address on my tax account was automatically changed with the filing of the fraudulent, electronic tax return in January 2005. After prodding and asking numerous questions as to why the IRS agent could not fully identify me during the call, but proceeded to give me account information because of my persistence, I learned that the address on my tax account was changed to the Pennsylvania address on the fraudulent return. At the time, I was told to submit IRS form 8822 to correct the address, with no timeframe for completion or special handling. Moreover, the IRS does not have the ability to flag victims' accounts, add a password or prevent unauthorized access to tax accounts by identities thieves with identifying information. I do not use predatory, for-profit tax preparers such as H&R Block to file my taxes. H&R Block employees throughout the country have been charged with identity theft crimes, among other things. As such, I specifically asked to have my tax account blocked from electronic filings by commercial, for-profit tax preparers such as H&R Block. I was told "no", that cannot be done. Thus, there are no safeguards for taxpayers whatsoever.

Lastly, form W2 is received by the IRS long after the April 15th deadline. In order to check for fraudulent wages annually with the SSA and IRS, I was told to call the IRS in August. That is when the IRS receives employer filings. Clearly, this should not occur. If tax documents are mandated to be mailed by employers to taxpayers no later than January 31st, then the filing with the IRS should happen simultaneously.

DMV

In my dealings with HSBC Bank to return the fraudulent tax refund amount to the IRS, the investigator indicated that fraud accounts for a small percent against the bank's revenue. Therefore, they are not likely to change the way "rapid refunds" or "refund anticipation loans" are processed through entities like H&R Block. Through my own investigation, I discovered that identity thieves obtained and used Pennsylvania Department of Motor Vehicles (DMV) identification to cash the fraudulent IRS check at a check cashing outfit, among other things. Therefore, merely asking tax preparers and financial institutions to request state issued identification is not enough. Identification must be authenticated at the point of service (financial transactions). This is done with national car rental agencies such as Avis, Budget and the like, as they are linked to DMV to validate licenses; when a driver rents a car, the driver's

license is swiped at the rental counter. Additionally, my license was swiped when I entered a government agency's building in NY several years ago. When I asked why, I was told they were checking for warrants, which was standard operating procedure prior to entering the building. Clearly, the technology not only exists, it has been deployed by the private and public sectors for several years.

DMV must be reformed nationwide. In my case, NYPD stated there is no way to determine if my information was used in other states to obtain DMV identification or licenses. If DMV in Pennsylvania had the ability to query state DMVs nationwide, like national car rental agencies do today, the fraudulent Pennsylvania DMV ID would not have been issued. The "one-SSN-one license/passport" rule has been circumvented by lax or non-existent agency controls. Moreover, the established standards for DMV documents remains severely compromised until or unless the process for issuing birth certificates is modified. Certified birth certificates can be obtained on the internet, by phone and fax with a debit or credit card. Clearly, if identity thieves can obtain credentials directly from DMV with fake birth certificates and social security cards, they can also obtain certified birth certificates to take over every aspect of a victims' identity and sell the authentic documents to criminals in the black market.

As I began to share my story, I realized that I was not alone; the NYPD detective that updated my police report was a victim of identity theft. In practice, criminals obtain identification and licenses from DMV across state lines, healthcare, insurance, public assistance benefits, employment, housing, cars, credit products and student financial aid, with ease. As a direct result, I must routinely visit the social security administration to check for and dispute fraudulent wages. It is with great frustration that I call the IRS several times per year to confirm that my tax account has not been accessed or altered by identity thieves.

RECOMMENDATIONS

- **Require employers to submit tax documents to the IRS on or before January 31st annually.**

Fraud can be minimized significantly if the IRS receives employer filings in January, with an eye toward flagging questionable electronic returns with address and employer discrepancies.

- **Address the problem.**

The IRS must coordinate with the U.S. Department of State (passport office), DMV nationwide and the SSA to identify fraudulent documents. It is critically important to develop a national standard for obtaining and authenticating DMV issued identification and passports, at the point of service (i.e. tax preparers authorized to submit returns to the IRS electronically); prosecute perpetrators to the fullest extent of the law; and to revise the "Real ID Act of 2005" as it pertains to identity theft.

To reiterate, the "one-SSN-one license/passport" rule has been circumvented by lax or non-existent controls. Moreover, the current standards for DMV issued documents remains severely compromised until or unless the process for issuing birth certificates is modified. Clearly, if identity thieves can obtain credentials directly from DMV with fake birth certificates and social security cards, they can also obtain certified birth certificates to sell to criminals.

- **Develop and execute streamlined procedures to assist identity theft victims.**

The staff in a newly created division of the IRS and/or Taxpayer Advocate's office, should be trained to assist identity theft victims to (1) file personal and business tax returns; (2) correct the record (i.e. address, fraudulent wages); (3) secure the tax account with a password; (4) coordinate with relevant financial institutions, federal and state agencies and; (5) return stolen money (tax refund) to the IRS.
In my case, the fraudulent return was processed through H&R Block and HSBC Bank (electronic "rapid refund") with fraudulent Pennsylvania DMV and W2 documents. The IRS was able to provide the banking information that the fraudulent return was routed to. Therefore, I worked with HSBC Bank's fraud department to issue a check to the IRS for further credit to my tax account. The IRS and state

regulators must take action against entities involved in perpetuating fraud; H&R Block has been sued more than once by individual and groups of Attorney Generals throughout the country (consumer fraud).

- **Modernize the IRS by investing in technology and eliminating earmarks.**

It is critically important that the IRS is at par with the private sector. The investment in technology can be financed in part by eliminating or placing a 4 year moratorium on earmarks. According to the Office of Management and Budget, Congress includes earmarks in appropriation bills - the annual spending bills that Congress enacts to allocate discretionary spending - and also in authorization bills. Given the fact that identity theft is the number one crime in America -- and the private sector earns billions from superfluous identity theft products and services, namely the credit bureaus Experian, Trans Union and Equifax -- the public welcomes a holistic approach to dealing with the identity theft crisis. This is a fair allocation of the funds, as it benefits all taxpayers, whereas earmarks do not.

- **All compromised tax accounts must be flagged and password protected by the IRS.**

Simply asking for account information that only the taxpayer should know (DOB, SSN, address, filing status, etc.) is insufficient, given the unfettered access to personal information online and offline.

- **Expedite the change of SSNs for identity theft victims.**

Identity theft victims have no way of determining if they are victims of criminal identity theft until their driver's license is suspended, they are detained by law enforcement (i.e. at the airport) and/or are falsely arrested. Once a criminal record is established, it is irreversible. Identity theft victims have no means to detect, expunge or seal criminal records once falsely accused of a crime as a direct result of identity theft. If it is proven that a victim's social security account, IRS tax account and/or DMV credentials have been compromised, victims should be allowed to change their SSNs upon request. This will invalidate the stolen SSN and eliminate further abuse of that number, abuse that cannot be detected by ordering credit reports. The SSA has the ability to document changes, so as not to interfere with SSA benefits.

It is with displaced anger that I contact DMV to check for warrants and other violations to prevent suspension of my driver's license or worse, false arrest, as was the case with Stancy Nesby. "From 2002 to 2004, Nesby was arrested seven times by five different police departments including being hauled off right in front of her terrified children."[1] In 2002, 36 individuals "including eight former Division of Motor Vehicle employees" in New Jersey, were charged with "racketeering, bribery, official misconduct, money laundering, theft, identity theft, forgery, falsifying records, tampering with public records and conspiracy."[2]

CONCLUSION

To suggest that individuals can "prevent" identity theft by being more careful, shredding documents or maintaining confidentiality, is false. In *United States v. Harrison,* (S.D. NY Dec.10, 2004), Harrison was charged with identity theft; Harrison had access to individuals' personal information through her position as a clerk at the NYC Human Resources Administration. For a fee, Harrison provided personal information to a third party, who used it to file false income tax returns.

In closing, I will make myself available to testify in person and to work with federal and state agencies to

[1]See KTVU News Video, *SAN FRANCISCO: Local Woman Struggles With Police Over ID Theft,* June 29, 2006, http://www.foxreno.com/news/9439467/detail.html

[2]See *Criminal Indictments Charge 36 Persons With Trafficking In Fraudulent New Jersey Driver's Licenses and Identification Documents*, June 24, 2002, http://www.state.nj.us/lps/dcj/releases/2002/dmv0624.htm

develop, execute and evaluate a holistic plan of action, work the "White House Identity Theft Task Force" has yet to do.

Respectfully submitted,

Keisha [redacted]

cc: IRS Commissioner Douglas Shulman

New York State Department of Motor Vehicles Commissioner David J. Swarts

New York State Senate
Senator Charles Fuschillo, Chair
Consumer Protection Committee

New York State Senate
Senator Hugh T. Farley, Chair
Banks Committee

New York State Assembly
Assemblywoman Audrey I. Pheffer, Chair
Consumer Affairs and Protection Committee

New York State Assembly
Assemblyman Darryl C. Towns, Chair
Banks Committee

2008 U.S. Presidential Candidates
(Re: White House Identity Theft Task Force)

○