AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 113–234

TAX FRAUD AND TAX ID THEFT: MOVING FORWARD WITH SOLUTIONS

HEARING

BEFORE THE

COMMITTEE ON FINANCE
UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

APRIL 16, 2013

Printed for the use of the Committee on Finance

U.S. GOVERNMENT PRINTING OFFICE

87–414—PDF WASHINGTON : 2013

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
RON WYDEN, Oregon
CHARLES E. SCHUMER, New York
DEBBIE STABENOW, Michigan
MARIA CANTWELL, Washington
BILL NELSON, Florida
ROBERT MENENDEZ, New Jersey
THOMAS R. CARPER, Delaware
BENJAMIN L. CARDIN, Maryland
SHERROD BROWN, Ohio
MICHAEL F. BENNET, Colorado
ROBERT P. CASEY, Jr., Pennsylvania

ORRIN G. HATCH, Utah
CHUCK GRASSLEY, Iowa
MIKE CRAPO, Idaho
PAT ROBERTS, Kansas
MICHAEL B. ENZI, Wyoming
JOHN CORNYN, Texas
JOHN THUNE, South Dakota
RICHARD BURR, North Carolina
JOHNNY ISAKSON, Georgia
ROB PORTMAN, Ohio
PATRICK J. TOOMEY, Pennsylvania

AMBER COTTLE, *Staff Director*
CHRIS CAMPBELL, *Republican Staff Director*

CONTENTS

OPENING STATEMENTS

	Page
Baucus, Hon. Max, a U.S. Senator from Montana, chairman, Committee on Finance	1
Hatch, Hon. Orrin G., a U.S. Senator from Utah	4

WITNESSES

Miller, Steven T., Acting Commissioner, Internal Revenue Service, Washington, DC	6
Porter, Jeffrey A., chair of the Tax Executive Committee, American Institute of Certified Public Accountants, and founder, Porter and Associates, Huntington, WV	7
Olson, Nina E., National Taxpayer Advocate, Internal Revenue Service, Washington, DC	9
LaCanfora, Marianna, Acting Deputy Commissioner, Retirement and Disability Policy, Social Security Administration, Washington, DC	11

ALPHABETICAL LISTING AND APPENDIX MATERIAL

Baucus, Hon. Max:	
Opening statement	1
Prepared statement	29
Hatch, Hon. Orrin G.:	
Opening statement	4
Prepared statement	32
LaCanfora, Marianna:	
Testimony	11
Prepared statement	34
Miller, Steven T.:	
Testimony	6
Prepared statement	41
Responses to questions from committee members	51
Olson, Nina E.:	
Testimony	9
Prepared statement	62
Porter, Jeffrey A.:	
Testimony	7
Prepared statement	91
Responses to questions from committee members	104
Wyden, Hon. Ron:	
Internal Revenue Service Office of Chief Counsel memorandum, dated July 8, 2011	109

COMMUNICATIONS

Consumers for Paper Options	117
International Association of Jewish Genealogical Societies (IAJGS)	122
LifeLock Inc.	129
National Conference of Insurance Legislators (NCOIL)	132
Records Preservation and Access Committee (RPAC)	138
Ryesky, Kenneth H.	146
Visa Inc.	150

TAX FRAUD AND TAX ID THEFT: MOVING FORWARD WITH SOLUTIONS

TUESDAY, APRIL 16, 2013

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

The hearing was convened, pursuant to notice, at 10:06 a.m., in room SD–215, Dirksen Senate Office Building, Hon. Max Baucus (chairman of the committee) presiding.

Present: Senators Wyden, Nelson, Cardin, Hatch, Grassley, Thune, and Isakson.

Also present: Democratic Staff: Amber Cottle, Staff Director; Mac Campbell, General Counsel; Lily Batchelder, Chief Tax Counsel; Ann Cammack, Tax Counsel; Tiffany Smith, Tax Counsel; and Tom Klouda, Professional Staff Member, Social Security. Republican Staff: Chris Campbell, Staff Director; Shawn Novak, Senior Accountant and Tax Counsel; and Jim Lyons, Tax Counsel.

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

The CHAIRMAN. The committee will come to order.

Before we begin, I think I can speak for every member of this committee in saying our thoughts and prayers are with the victims of the Boston Marathon bombing and with the families of all those impacted by that horrible tragedy.

We are also grateful for the brave first responders on the scene who undoubtedly saved countless lives. Acts of violence such as this clearly are not tolerated in our country, and all of us will work together to make sure the perpetrators are brought to justice, while we offer our condolences and sympathy to those who are more directly affected.

The Czech writer and politician Vaclav Havel once said, "I have preserved my identity, put its credibility to the test, and defended my dignity. What good this will bring to the world, I do not know. But for me it is good."

Our identity represents who we are. It represents our morals, our culture, our sense of worth. It represents, as Havel said, our credibility and our dignity. When stolen from us, it can have devastating consequences. Identity theft is a serious problem. It is growing at epidemic proportions, especially tax-related identity theft.

According to the IRS Taxpayer Advocate, tax-related identity theft jumped more than 650 percent between 2008 and 2012. Last year alone there were 1.8 million incidents of identity theft and

fraudulent refunds. One of the latest victims is Kipp Saile, a 48-year-old horseback outfitter in Pray, MT, a tiny town just outside Yellowstone National Park.

Like many Montana communities, everyone in Pray knows their neighbor. Doors are left unlocked, and the only threat of crime involves the possibility of a bear stealing your catch from the Yellowstone River. It is the last place you would expect to find a case of identity theft.

Yet earlier this year, Kipp was in the process of refinancing his home when he got a call from his tax preparer. There was a serious problem, he said. When the preparer tried to submit Kipp's tax return to complete his refinancing, it was rejected by the IRS.

According to IRS records, Kipp had moved more than 2,000 miles to Maryland, taken up a new wife, and no longer cared for his kids. In reality, of course, Kipp lived on his 10 acres in Pray with his wife of 11 years, Heidi, and their three children. Someone had stolen Kipp's identity and filed a false tax return using his Social Security number.

That is where the nightmare began. Kipp has since been forced to spend every day trying to repair the damage to his name and credit. Needless to say, it has been a stressful experience. It has cost Kipp many a sleepless night and quite a bit of money. The refinance has been put on hold, costing him an additional $500 a month he would have saved with the lower mortgage.

Instead of helping Kipp clear up this mess, the IRS has made a bad situation even worse. Kipp has been told twice by IRS employees that he was not defrauded, the U.S. Government was. At least one IRS employee hung up on Kipp, cut him off, and was rude. He hung up on Kipp while he was trying to make his case.

I find that outrageous, and I will not stand for a Montanan, or any American taxpayer, to be treated with that kind of disrespect by an IRS employee or any agency employee, employees who are supposed to be serving the public.

I am going to say this very clearly, Mr. Miller: never forget that you and everyone else at the IRS work for Kipp Saile and all American taxpayers. Your job is to serve them. They are the employers; you are the employees. I certainly hope this was an isolated incident and does not reflect the type of service provided by the IRS. But there is no excuse for even one rude employee like this, and I intend to find out what you are doing to make sure this type of behavior is not repeated.

It is critical that the IRS be ready and equipped to handle cases like Kipp's because they are increasingly common. We have all seen the stories in the newspapers and on TV about ID theft. Just last week, *USA Today* highlighted some of the most egregious examples of tax ID fraud, like a case where one address in Michigan was used to file 2,137 tax returns. There was another case where a single bank account was used to receive 590 direct deposit refunds from the IRS, totaling more than $900,000.

In recent congressional testimony, the IRS reported that they had identified more than 900,000 fraudulent returns and stopped more than $6.5 billion in fraudulent refunds in 2011, but that was only the tip of the iceberg.

The Treasury Inspector General for Tax Administration recently reported that another 1.5 million fraudulent returns went undetected in 2011, potentially allowing $5.2 billion in refunds to be paid. The IG estimated that if tax identity theft were not addressed, it could cost the IRS $21 billion in fraudulent refunds over the next 5 years.

Enough is enough. It is time to act. Three weeks ago, members of this committee were briefed on tax reform options that included proposals to help combat tax fraud and tax ID theft. Senator Nelson, joined by Senators Cardin, Schumer, and Feinstein, introduced comprehensive tax fraud legislation last week. I commend them for that. I am pleased that the administration has included several significant tax fraud prevention proposals in its fiscal year 2014 budget.

This includes limiting access to death records and omitting Social Security numbers on wage statements, but there is still much more that can be done. We know tax fraudsters have easy access to taxpayers' Social Security numbers through online databases, hospitals, and other businesses that store personal information. We need tougher controls on access to private information, but it needs to be done efficiently without adding more paperwork to the process.

We know that fraud is easier to detect when the IRS can match a W–2 filed by an employer to a tax return before issuing a refund. Right now that is not happening. We need to cut through the red tape and ensure this information gets to the IRS quickly.

We also know that too often it can be the tax return preparers themselves who are the identity thieves. Proper oversight by the IRS can help prevent this, but we face obstacles. The IRS was handed a major setback recently when the Federal court ruled against their authority to regulate some tax return preparers. The case *Loving v. IRS* is ongoing, and I am hopeful that the IRS will succeed on appeal, otherwise taxpayers will not be able to know if they are using a reliable return preparer.

I will be asking for an update on the status of this. We need to consider whether legislation is necessary to protect taxpayers from fraudulent preparers. This committee outlined several ideas recently to reimpose tax preparer regulations, and I encourage you to look at those ideas as part of our tax reform option papers.

I also want to hear today how the IRS is utilizing the tools they already have. *USA Today* recently stated that the IRS is "losing the identity theft fight" and criticized the IRS for taking too long to resolve fraud cases. According to the National Taxpayer Advocate, it takes an average of more than 180 days to close cases. That is unacceptable. The IRS needs to step it up and improve the way it handles tax ID theft once cases are identified.

Victims of ID theft, people like Kipp Saile, are forced to put their lives on hold while their cases languish in red tape. IRS needs to speed up prosecution through better communication with Federal, State, and local law enforcement, and this committee is committed to protecting the American taxpayer. I am hopeful that we will be able to work together to move forward with legislation to stop tax ID theft.

We owe that to Kipp Saile and all the victims of identity theft, and to all American taxpayers who pay their bills properly and on time and are obviously quite put out when too many others do not.*

[The prepared statement of Chairman Baucus appears in the appendix.]

The CHAIRMAN. Senator Hatch?

OPENING STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM UTAH

Senator HATCH. Well, thank you, Mr. Chairman. I agree with your statement. Before I begin, I just want to say that my prayers go out to the city of Boston, especially for the families of those who lost their lives and have been very seriously hurt and injured. I wish everyone who was impacted by this tragedy a very swift and peaceful recovery, to the extent that that can happen.

I also want to thank you, Mr. Chairman, for holding this important hearing. Each year the Finance Committee holds a hearing around the end of the tax filing season. In the past, these hearings have provided unique insight into the issues faced by the American taxpayers, as well as some of the overall problems we have with our Nation's tax system. The chairman has announced some of them.

The subject of this year's hearing is the rapidly growing crime of tax fraud by identity theft. This is a serious matter and deserves our careful attention. Two of my colleagues, Senator Nelson and Senator Crapo, should be commended for their efforts in this area. Their subcommittee, the Subcommittee on Fiscal Responsibility and Economic Growth, has held two hearings on this topic over the last 2 years.

In addition, this was an important topic of conversation at last year's tax filing season before the full committee. I share the concerns of many throughout our country regarding tax fraud by identity theft. From 2010 to 2011, the number of these crimes nearly tripled, going from about 440,000 to 1.1 million.

Two senior members of my Finance Committee staff know this issue very well, as they have been victims of tax fraud by identity theft. In both cases, criminals obtained their Social Security numbers, filed fraudulent returns, and collected refunds.

For both staffers, this began a nightmarish scenario in which they had to spend days on the phone and filling out paperwork just to be able to file their own tax return. In the end, they have to live with the fact that their Social Security numbers are out there, and they can only hope that they are not used to commit another fraud.

So I want to thank our four witnesses for coming to talk to us today about this troubling issue, and I assure you we are listening very carefully.

When it comes to dealing with tax fraud and identity theft, I understand that the IRS has adopted a 3-pronged approach. The first prong is prevention, which means stopping this type of tax fraud

---

*For more information, *see also*, "Present Law and Background Information Related to Selected Tax Procedure and Administration Issues," Joint Committee on Taxation staff report, April 15, 2013 (JCX–9–13), *https://www.jct.gov/publications.html?func=startdown&id=4515*.

from being successful in the first place. Clearly, given the prevalence of this crime, much more work needs to be done in this area.

The second prong is providing taxpayer services for those who have been the victims of identity theft. This is a significant focus of the IRS, but it appears that the agency is falling woefully short in some instances. For example, an audit by the Treasury Inspector General for Tax Administration sampled 17 different identity theft cases and found that the average time it took for these cases to be resolved was 414 days. Now, that is simply too long a wait for taxpayers who have been the victims of identity theft, and I am hoping that we can discuss ways to cut that wait time down during today's hearing.

The third prong of the IRS's approach is catching and convicting the criminals who have committed these crimes. This is a critically important step. If we can step up enforcement, many would-be criminals would likely decide that it is not worth the risk to commit these crimes. I think we ought to have very stiff penalties in these cases, and, frankly, they ought to be enforced.

I am interested in hearing more about the IRS's efforts to follow this 3-pronged approach, what successes they have had, and what challenges they are still facing. I particularly enjoyed meeting with you, Mr. Miller, yesterday. It was a good meeting. That is why I am glad that we have you top IRS people with us here today. Acting Commissioner Steve Miller, we are grateful that you are here today. I know that you are taking this seriously.

In addition, I want to know what other steps could be taken to prevent these crimes, assist the victims, and improve enforcement. I believe all of our witnesses here today will be able to address some of these questions. While tax fraud identity theft is the major focus of this hearing, we will also discuss general issues associated with the tax filing season.

This year, as with every year, taxpayers face a number of issues and obstacles as they try to file their returns. We clearly need to do better in providing assistance during what can be a very difficult time for many of our citizens.

For example, at last year's hearing I noted that the IRS's goal of answering 61 percent of taxpayers' service calls was unacceptable. I am glad to see this year that the IRS set a significantly higher goal. That said, I still think more can be done to improve taxpayer service.

I hope we can have a full and informative discussion of these issues during today's hearing. Once again, I want to thank the distinguished Senator from Florida and others for the work that they have been doing in this area, and I want to welcome our witnesses.

Mr. Chairman, I look forward to this very important hearing, and we appreciate you folks being here with us today.

The CHAIRMAN. Thank you, Senator.

[The prepared statement of Senator Hatch appears in the appendix.]

The CHAIRMAN. I would like to introduce our four witnesses. First is Mr. Steven Miller. Mr. Miller is Acting Commissioner of the IRS. Next to Mr. Miller is Ms. Nina Olson, the National Taxpayer Advocate. The third witness is Mr. Jeffrey Porter, who is sitting next to Mr. Miller. He is chair of the Tax Executive Committee

for the American Institute of Certified Public Accountants. Finally, we have Ms. Marianna LaCanfora, Acting Deputy Commissioner of Retirement and Disability Policy for the Social Security Administration. Did I pronounce your name correctly?

Ms. LACANFORA. Yes. Thank you.

The CHAIRMAN. Thank you.

Mr. Miller, you are first. You know the drill. Speak for about 5 minutes. Your statements will be in the record.

STATEMENT OF STEVEN T. MILLER, ACTING COMMISSIONER, INTERNAL REVENUE SERVICE, WASHINGTON, DC

Mr. MILLER. Thank you, Chairman Baucus, Ranking Member Hatch, members of the committee. Thanks for the opportunity to update you today. Obviously, Chairman Baucus, the treatment that Mr. Saile got was not acceptable and not up to what we hope are our standards, and we will look into that.

The CHAIRMAN. I appreciate that. Thank you.

Mr. MILLER. While I will spend most of my time today discussing the future, I first want to touch on where we are. The agency has more than 3,000 employees working on identity theft. Last year, we stopped $20 billion in fraud. You had talked about 2011. In 2012, $20 billion in fraud before it went out, up from that $6 billion the year before. Our ability to stop bad refunds has improved this year as well.

In addition, the number of criminal investigations continues to rise, with more than 800 so far this year. Finally, we are making progress on getting victims their refunds. It is still slow, Mr. Chairman, but we are making progress. We have closed more than 200,000 of these cases since the beginning of this calendar year, and for the first time, over the last couple of months, we are closing more than we are getting in. So, our inventory is getting under control.

All this is not without cost. We spent almost $330 million out of our declining budget on these matters in 2012, so in my mind we are better, but our work is not done. We need to get better still.

What I would like to do now is walk through where we need to be to take the next major step in fighting identity theft. The barriers to get there include the proliferation in the theft and availability of SSNs, the sheer volume and complexity of the cases before us, available IRS resources—and in particular resources for technology updates—as well as third-party information reporting, and our own business processes. We have started work in several of these areas, but much more remains to be done.

Here is where we need to be in the future. To illustrate, let us follow how my return would move through our system. First, at the time of filing before the return enters our system, I should have to authenticate who I am in a robust manner, even before it gets in to the IRS. This should happen regardless of how I file. The issue is how to do this. Do we, for example, use out-of-wallet questions, personal information that is known to me but is tough for an identity thief to steal or track down?

After authentication and as my return enters the system, the IRS has to employ a set of flexible filters and tools that allow a more informed decision on whether to issue a refund. That decision

must be based on a wider array of information than is available to us today.

Here, let us talk about intelligent matching. First, the IRS needs to validate that I am who I say I am. We need to do this by using all the data in our systems, as well as other data that is not currently available to us, on a timely basis, at least.

So, for example, we need to look at my return and ask, do I look like the same Steve Miller who has filed in the past? Do I live in the same place, work at the same place, have the same family, et cetera? Is the information on my return consistent with other data we are receiving? So some of the data needed is historical, and some is current third-party data.

Historical data we may have already, though it may not always be available to us on a timely basis. But in this future state, we also need to at least have some third-party data to validate both my identity and other items on my return.

In this world, the IRS may have my W–2, certain 1099s, et cetera, at the time the IRS makes the determination of whether a refund is due to me and whether the amount claimed is correct. Issues to discuss here include the need for improved technology, the timing of data receipt, burden on reporting entities, and the need for some taxpayers to have a fast refund.

Next in the future vision is how we deal with victims. Here, we need better coordination internally, and, more importantly, we need a better solution for those like Mr. Saile, who is the second one to file with us. Right now, second filers are forced to submit a paper return, and they face a long wait.

We need to get to a point where we take that second filer in electronically and we prove the identity more efficiently, and we need to have an improved system to issue an Identity Protection PIN, which we could talk about. The key issue again here is technology. Existing technology does not get us there.

There are other areas to discuss and many important, far-reaching questions that merit discussion about the future and shape of tax administration. These questions should be considered not just inside the IRS, but with the tax community, law enforcement, as well as you in Congress and taxpayers.

As I describe for you a preferred future for fighting identity theft, please recognize that improvements are neither immediate nor are they possible without resources. I will ask for your support for the 2014 budget which includes additional funding on this issue, as well as several important proposals on identity theft.

Thanks again for the opportunity to be present.

The CHAIRMAN. You bet. Thanks, Mr. Miller.

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

The CHAIRMAN. Mr. Porter, you are next.

STATEMENT OF JEFFREY A. PORTER, CHAIR OF THE TAX EXECUTIVE COMMITTEE, AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS, AND FOUNDER, PORTER AND ASSOCIATES, HUNTINGTON, WV

Mr. PORTER. Good morning, Chairman Baucus, Ranking Member Hatch, and members of the committee. My name is Jeffrey Porter, and I am the chair of the American Institute of CPAs Tax Execu-

tive Committee and a sole practitioner at Porter and Associates in Huntington, WV. On behalf of the AICPA, I am pleased to have the opportunity to testify today.

An important issue of concern for our members is identity theft. In mitigation of this issue, the AICPA appreciates the IRS's recent issuance of proposed regulations which authorize filers of certain information returns to truncate a taxpayer's identifying number.

However, unfortunately there are some statutory limits placed upon the Service's ability to expand their truncation initiative. For example, employers are required to provide employees a W–2 with their full Social Security number. We urge Congress to permit truncation of Social Security numbers on all copies of W–2s other than those filed with the Social Security Administration. We also urge Congress to consider expansive legislation to allow truncation of Social Security numbers on all types of tax forms and returns provided to a taxpayer, employee, or other recipient.

Now I would like to share our feedback on this year's tax filing season. Overall, it was an extremely challenging and compressed filing season due to the late enactment of legislation and the resulting delay in the release of 31 tax forms.

Since the IRS could not accept tax returns that included certain forms until February or early March, our members essentially lost the first half of their filing season. Nevertheless, we believe the IRS did an outstanding job under difficult circumstances. They maintained an open dialogue with stakeholders and were responsive to our concerns.

Earlier this year, we submitted a letter to Acting Commissioner Miller on the delayed release of forms. Within days, the IRS issued a notice which provided critical relief requested from late payment penalties.

Unfortunately, the filing season was also a challenge due to the late issuance of corrected 1099s. Generally, a 1099 must be furnished to taxpayers by February 15th; however, brokerage firms can amend a 1099 at any time. Over the last few years, we have noticed more brokerage firms issuing corrected 1099s, sometimes issuing multiple corrected forms on the same account. These forms create anxiety, confusion, and, for some taxpayers, an increase in tax preparation fees.

As a result, many taxpayers now have a tendency to wait until they have received their anticipated corrected 1099s before providing records to the CPA. In order to streamline the tax return reporting process for both the government and taxpayers and to minimize the need for amended tax returns, we suggest you consider legislation that would permit taxpayers to report de minimus changes in their income from a corrected 1099 in the year of receipt.

Another area of interest for our profession is the IRS's tax return preparer program. The AICPA has always been a steadfast supporter of the Service's goals of enhancing compliance and elevating ethical conduct. We generally support their program, including the registration of paid tax return preparers and the issuance of preparer tax identification numbers; the expansion of Circular 230 over all paid preparers; the creation of a basic continuing education and competence program geared towards the unenrolled preparer

community; and the IRS's mitigation of any taxpayer confusion regarding the qualifications of different paid preparers.

Another important issue is the reform of penalties. Because the success of our system depends upon voluntary compliance, penalty provisions should be carefully crafted by Congress and sensibly administered by the Service to ensure that penalties deter bad conduct without deterring good conduct or punishing the innocent.

Targeted, proportionate penalties that clearly articulate standards of behavior and are administered in an even-handed and reasonable manner encourage voluntarily compliance with the tax laws.

On the other hand, over-broad, vaguely defined, and disproportionate penalties, particularly those administered as part of a system that automatically imposes penalties or that otherwise fails to provide basic due process safeguards, creates a perception of unfairness that is likely to discourage voluntary compliance.

Finally, we appreciate the committee's important consideration of tax reform and potential solutions. We have consistently supported tax reform simplification efforts, because we are convinced that such actions will reduce taxpayers' compliance costs, encourage voluntary compliance, and facilitate enforcement actions.

To name a few, we support the repeal of the Alternative Minimum Tax, the harmonization of education incentives, the enactment of consistent definitions in the code, the repeal of unused provisions, and the simplification of the kiddie tax rules. We also believe in the simplification and harmonization of retirement planning vehicles. We have more extensive thoughts on tax reform, tax reform due dates, and information reporting in the written comments submitted to this committee.

Thank you again for the opportunity to testify. I will be pleased to answer any questions you may have.

The CHAIRMAN. Thank you, Mr. Porter. I presume you submitted all those recommendations for simplification and changes to this committee as we work on tax reform.

Mr. PORTER. Yes, sir.

The CHAIRMAN. We need lots of help, frankly, to make sure we do it right. All right. Thank you.

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

The CHAIRMAN. Ms. Olson?

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

Ms. OLSON. Chairman Baucus, Ranking Member Hatch, and members of the committee, thank you for inviting me to testify today about tax-related identity theft. Before I begin, I want to commend you for the excellent tax reform options paper the committee staff compiled last month and urge you to move forward with comprehensive tax reform and a taxpayer bill of rights.

I also want to make you aware of my concern that cuts to the IRS budget since 2010, including but not limited to sequestration, are impairing the IRS's ability to serve taxpayers and are self-defeating as a deficit-reduction measure. Almost surely the reduction in revenue collection will ultimately exceed the short-term budget savings.

On the subject of identity theft, let me start by emphasizing the most important impact for most victims: delayed refunds. Apart from the time and obvious frustration involved in having to prove one's own identity, a taxpayer generally will not receive his or her refund until the case is fully resolved.

So far this filing season, 84 percent of all individual returns processed have resulted in refunds, and the average refund amount has been nearly $2,800, so longer case resolution times often translate into financial inconvenience, or even hardship. Some identity theft victims also experience consequences when other Federal agencies or private businesses rely on IRS data.

For example, the IRS generally will not release account transcripts while an identity theft case is pending, so students applying for financial aid and homeowners applying for a mortgage or refinancing may face additional obstacles. That is why prompt case resolution is so important.

Yet, cases are not being resolved promptly, nor do taxpayers have a single point of contact to work with, nor does the IRS even have a reliable way of measuring service-wide cycle time on identity theft cases.

The IRS recently created 21 separate specialized units to handle different types of identity theft problems, which may be helpful, but, when a case involves multiple issues, one IRS entity should oversee the case to make sure the problems are handled in a coordinated manner. The IRS seems to believe that relatively few cases require involvement by multiple functions. I disagree. Within the Taxpayer Advocate Service, 94 percent of our identity theft cases have multiple issues.

Similarly, TIGTA reviewed a judgmental sample of 17 identity theft cases for an audit conducted last year and found that the IRS had opened 58 cases separately to resolve these victims' accounts, an average of nearly three and a half cases per victim. The average cycle time for those cases was well over a year.

IRS data suggests its workload continues to grow at a rapid clip. The IRS had more than 1.25 million identity theft cases in inventory at the end of February, more than 5 times as much as a year ago when the volume was less than 235,000 cases. After years of so-called IRS reengineering efforts, victims are still experiencing unacceptable delays.

From an administrative standpoint, there are several steps the IRS can take to improve victim assistance. The IRS should create a strong centralized unit so ID theft victims with multiple issues do not have to deal with multiple functions to get complex problems resolved. The IRS should analyze its procedures to identify ways to reduce cycle time.

The Taxpayer Advocate Service generally is able to resolve identity theft cases in about 3 months, and there is no reason why the IRS should need from 6 months to over a year to do so. The IRS should do a better job of keeping victims informed of the status of their cases while they are in progress, and promptly issue refunds when it has identified the correct taxpayer, instead of waiting until case closing.

From a congressional standpoint, I believe several steps could make a difference. First, I recommend that Congress consider what

needs to be done to enable the IRS to receive and process information returns, like forms W–2, before it processes income tax returns and issues refunds. If the wage and withholding on a tax return had to match the numbers filed by employers on forms W–2, identity thieves would have a much harder time.

Second, I recommend that Congress restrict access to the Death Master File which provides a means of access to taxpayer-identifying information that can further tax fraud. Third, I recommend that you enact restrictions on the use and disclosure of taxpayer return information shared by the IRS with State and local law enforcement authorities.

Finally, I have long advocated for the regulation of Federal tax preparers for many reasons, one of which is that it will reduce the incidents of fraud. If the Court of Appeals for the D.C. Circuit ultimately invalidates the Treasury's preparer regulations, I encourage this committee to do what it has done on two previous occasions and approve legislation explicitly authorizing the IRS to regulate in this area.

I appreciate the opportunity to testify today and would be happy to answer your questions.

The CHAIRMAN. Thank you, Ms. Olson.

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

The CHAIRMAN. Ms. LaCanfora?

STATEMENT OF MARIANNA LaCANFORA, ACTING DEPUTY COMMISSIONER, RETIREMENT AND DISABILITY POLICY, SOCIAL SECURITY ADMINISTRATION, WASHINGTON, DC

Ms. LACANFORA. Chairman Baucus, Ranking Member Hatch, and members of the committee, thank you for inviting me to this important hearing on tax fraud, tax ID theft, and tax reform. I will discuss the death information that we maintain to administer Social Security programs and our role in the wage reporting process.

I am Marianna LaCanfora, the Social Security Administration's Acting Deputy Commissioner for Retirement and Disability Policy. At Social Security, we are responsible for administering some of the Nation's most important and most successful programs. We take great pride in helping the American people obtain the benefits to which they are entitled. We are also committed to protecting the sensitive data that we collect and maintain.

The President's fiscal year 2014 budget includes four SSA-related legislative proposals that would enhance our ability to combat fraud, curb improper payments, and improve our wage reporting process.

I would like to briefly explain the history behind one of these legislative proposals, which would restrict access to the Death Master File, or the DMF. Since Social Security began in the 1930s, we have collected death information from funeral homes, States, and other sources to timely stop paying beneficiaries who have died. Each year, we receive about 2.5 million reports of death. When we receive this information, we update our records, stop benefits as appropriate, and, in some cases, start paying benefits to surviving spouses and young children.

People eventually became aware of our collection of death records. In 1978, Ronald Perholtz filed a lawsuit under the Free-

dom of Information Act, or FOIA, to gain access to the death records in our files. The Department of Justice advised us that we could not withhold the data requested under FOIA.

As a result, we entered into a court-approved consent decree requiring us to disclose death records regularly. In time, because we began to receive more and more requests for death information, we contracted with the Department of Commerce's National Technical Information Service to distribute the Death Master File.

Recent media reports have stated that criminals use the DMF information to perpetrate tax fraud. While death data can be a very valuable tool to prevent fraud, we must strike a balance that allows legitimate uses of the data while also preventing misuse. That is why we believe the law should be changed to stop wrongdoers from obtaining our death information.

The legislative proposal would delay the release of a deceased individual's information on the DMF for 3 years after he or she dies. Only private entities that the Commissioner certifies as having a legitimate need for the information would receive the DMF immediately.

At the same time, the proposal would expand Federal agencies' access to death information for additional purposes, such as law enforcement and reducing improper government payments. We look forward to working with Congress on this legislation. This budget includes another proposal that would permit us to share our prisoner information to help other agencies reduce improper payments.

I would like to briefly touch upon the wage reporting process. We collect wage reports to ensure that workers receive Social Security credit for their work. We also use this information to calculate benefit amounts. On a daily basis, we provide it to the IRS for tax administration.

The President's fiscal year 2014 budget includes two proposals that would enhance the wage reporting process while also helping to prevent fraud and error. One proposal would require more employers to file electronic wage reports, which are far more accurate than paper. The second proposal would restructure the Federal wage reporting process by requiring employers to report wages quarterly rather than annually. Increasing the frequency and timeliness of wage reporting would enhance the ability to detect fraud and curb improper payments.

Again, thank you for the opportunity to describe our efforts in this area. I would be happy to answer any questions you may have.

The CHAIRMAN. Thank you, Ms. LaCanfora.

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

The CHAIRMAN. I have two questions, really. First is, with a 3-year delay in releasing the deceased Social Security numbers, can't the IRS have access to that information and match any refund requests or returns filed with the IRS against those to find out whether that person is actually alive? Maybe you, Mr. Miller, can answer that question.

Mr. MILLER. So, we do receive the Death Master File currently. We do mark accounts in two ways. Those who have recently passed, their estate has to file a tax return with us, so they have a filing requirement. We cannot simply lock that account.

We do tag it so that we can judge whether it is a proper estate tax return or not, and we capture quite a few of those in our filters. With respect to those who have passed more than a couple of years ago, we do lock down their account so that people cannot use those. We have locked down more than 11 million of those accounts.

The CHAIRMAN. So how confident are you that people are not ripping taxpayers off by fraudulently using these Social Security numbers, that is, numbers of people who are deceased? How confident are you that there is not much leakage there anymore?

Mr. MILLER. I am quite sure there is some leakage, Senator.

The CHAIRMAN. Where would it be? What is the flaw? Where are the cracks in the system?

Mr. MILLER. So—and I would open it to my colleague from SSA as well—the system is only as good as the reporting to SSA is, and only as timely as the reporting to SSA is. These are not necessarily all coming from the DMF. People are stealing from funeral homes, from hospitals, so they may be utilizing those numbers in advance of our ability to load them in our system.

The CHAIRMAN. What about those other sources; what are you doing about that: funeral homes, hospitals, et cetera?

Mr. MILLER. So, we do not have the authority or the capabilities to police the use of Socials. All we can do is try to educate.

The CHAIRMAN. If you had the authority, how important would that be to your enforcement?

Mr. MILLER. I do not know whether that would be the IRS that should have that authority or whether others should have that authority. It is clearly a gap in the system. Someone needs to educate and make clear that these Socials need to be protected. We are trying to do that, and we are also trying, as you heard, in terms of the administration's proposal, to try to get fewer of those SSNs floating around in the system.

The CHAIRMAN. I would be interested in your reaction, and maybe others on the panel in my limited amount of time, to doing electronic filing. California is setting up a pilot program, as I understand it, where the State just sends you your return, and it is all filled out for you. I am trying to find some ways to use electronic systems to create more efficiency. So, if you could just comment a little bit on what we could do there.

Mr. MILLER. I think, if I am understanding the question, Mr. Chairman, we are talking about California's—what is called the Ready Return, or something of that nature.

The CHAIRMAN. Yes. Right.

Mr. MILLER. You would have to talk to California about how well it is doing. My understanding is it works, but for a limited number of individuals. We have actually worked with the software community, and they are partners in doing this. I am not sure that that is an answer to identity theft. Whether we want to go that way or not is a different question in terms of burden on the taxpayer, but I am not sure at all that that is going to be——

The CHAIRMAN. Just off the top of your heard reaction, is that something worth pursuing, the Ready Return approach?

Mr. MILLER. Depending on where it would be in line of my priorities, Mr. Chairman, but it is not at the top of my priorities, no.

The CHAIRMAN. And why not?

Mr. MILLER. Because we have quite a few other things on our plate right now.

The CHAIRMAN. Yes. Others? Is there potential? Let me ask Mr. Porter, Ms. Olson.

Ms. OLSON. Well, in my annual report, what we recommended for enforcement reasons is that the IRS needs to get W–2 and 1099 data very early so it can do some of the protections for identity theft and fraud, and then, once we have that data, we should make that available to taxpayers so that they can download it into the software programs that they are purchasing or that they can give it to their preparers so we do not miss a 1099 or a W–2 somewhere. Or we recommend that the IRS create a return itself whereby taxpayers could download that information. For a small category of taxpayers, that return would be it, because they only have W–2 information.

The CHAIRMAN. Right. Right. My time is expiring.

Ms. OLSON. But for many others——

The CHAIRMAN. My time is expiring. But, Mr. Miller, very briefly, what are your number-one and your number-two priorities?

Mr. MILLER. My number-one priority just finished up last night.

The CHAIRMAN. Well, that is history then. What is it now? [Laughter.]

Mr. MILLER. Making sure those returns finish their winding through and people get their refunds, Mr. Chairman. That is number one.

Number two is the other legislative things we have in front of us, including the foreign account work we have, the health care act work that we have, and identity theft. Those are all in the same category.

The CHAIRMAN. All right. Thank you. Thank you.

Senator Hatch?

Senator HATCH. Thank you, Mr. Chairman.

Ms. Olson, if a criminal has the taxpayer's name and Social Security number, it may be enough to file a fraudulent return seeking a refund. Now, identity theft victims now receive an additional layer of security to prevent the fraud from happening to them again. Would adding a similar, additional layer of security for all taxpayers be an effective way to prevent tax fraud related to identity theft?

Ms. OLSON. I think that that is something worth looking into. People who e-file already have to answer certain questions, information off the last year's return. What Acting Commissioner Miller was talking about, some of these out-of-wallet questions, things that we are familiar with—what was the name of your elementary school, your first pet, et cetera—are getting more accepted in doing business and may be easier for taxpayers to answer.

I would also make a comment about something Mr. Miller referred to earlier about funeral homes and hospitals. I often wonder why they need Social Security numbers in the first place, why those numbers are available to these entities. Why are they asking for them? I think that that is something worth looking at, the proliferation of people asking for Social Security numbers where there is no overriding tax need, for example, for giving that information.

Senator HATCH. All right. Thank you.

Mr. Miller, are refundable tax credits an element of the income tax system that make it easier for criminals to obtain fraudulent refunds, and are they more susceptible to fraud than non-refundable credits?

Mr. MILLER. I do not think we can crowd all refundable credits into one pile, Senator. I think that it is clear that where a refundable credit represents a large hunk of money, that that becomes a target, a natural target for thieves.

That would be true of any credit, but especially of a refundable credit where there is no natural break on its utility. It really depends on the nature of what information we have to validate that credit at the time. I think that is more important than whether it is refundable or not.

Senator HATCH. Well, as you know, some have advocated a return to more paper filing as a way to combat tax fraud through identity theft. However, would going to more paper tax return filings really reduce this crime?

Mr. MILLER. We do not think so, Senator. First, we still see a goodly amount of fraudulent returns coming in on paper. Second, whether they come in on paper or whether they come in electronically, those returns and that information are going through the same system.

So what we would have is a delta between something that costs us about 17 cents to process, that is an electronic return, and $3-plus for a paper return for, in our mind, not necessarily much benefit in terms of cutting down on fraud.

Senator HATCH. I see.

Mr. Porter, as a longtime professional tax practitioner, you have undoubtedly dealt with many cases where the IRS has assessed penalties. Penalties can be waived in some cases where the taxpayer can demonstrate "reasonable cause." Do existing reasonable cause exceptions adequately protect both taxpayers and the government, and where is there room for improvement in this area?

Mr. PORTER. Well, we have concerns about areas where there is not reasonable cause, where the reasonable cause exception is not allowed. So that is one area we are concerned about. Our concerns in the area where there are reasonable cause exceptions deals with really the subjectivity with which the rules are applied. As we all know, the tax code is extremely complex, and taxpayers many times will make foot faults that are unintentional, so we just believe that the subjectivity issue of how we decide whether they are or are not abated is the issue.

Senator HATCH. All right.

This is for all three of you. The IRS's planned regulation of paid tax return preparers is currently on hold. The IRS lost on its appeal in a recent District Court case that ruled that the IRS does not have the authority to regulate tax return preparers.

How important is the IRS's ability to regulate tax return preparers in the battle to combat tax fraud, tax refund fraud for instance?

Mr. MILLER. If I could start out, Senator. We think it is remarkably important. First, we have worked with the Department of Justice, and we are appealing the District Court case. We hope to get an answer this calendar year. Yes, we think it is vital. We think

it is vital to our ability to allow the public some confidence that the return preparer whom they are selecting meets certain basic competencies. So, we find it very important.

Senator HATCH. Mr. Porter?

Mr. PORTER. We have consistently supported the IRS and their program to register tax return preparers and provide ID numbers, and the expansion of Circular 230. We agree that we think it provides the taxpayer a level of confidence to know their preparer has at least a basic level of competence, and it allows the IRS the ability to track preparers and to see the type of returns that they are preparing and potentially be able to spot fraud issues early on.

Senator HATCH. All right. Ms. Olson?

Ms. OLSON. I personally have over 50 taxpayer assistance orders sitting on my desk that are in the process of being issued to Mr. Miller over there on my right, where the taxpayers have been the victims of preparer fraud.

The preparers have taken their identity or filed unauthorized returns and had the refunds of significant amounts of money—as much as $5,000—deposited into their personal accounts. We are dealing right now with the fall-out of the legitimate taxpayer trying to file a second return, a real return, and getting their refund back from us.

When I see return preparers in massage parlors and return preparers in dog grooming locations, I am not saying that they should be shut down, but I am saying that they should be required to demonstrate their competency to prepare returns. That is the environment that we have today, absent this regulation, that folks are just hanging up their shingle without any qualifications whatsoever.

Senator HATCH [presiding]. All right. Thank you all.

Senator Grassley?

Senator GRASSLEY. Yes. Mr. Miller, recent reports indicate that the IRS has taken a position that it can access taxpayer e-mails without warrant under the Electronic Communications Privacy Act. While that law does allow Federal agencies to obtain electronic communications from a remote computing service without a search warrant, provided that they are older than 180 days, this position is contrary to the 6th Circuit decision in *Warshak*.

In that case, the court held that the search warrant is necessary to obtain any content of an e-mail, regardless of age. It is my understanding that the Department of Justice has extended this policy to all circuits. So my question is, why is the IRS taking a more aggressive posture under that law than the Justice Department has applied for all agencies, or applied to all circuits?

Mr. MILLER. Well, Senator Grassley, the short answer is, we are not taking that position. We follow *Warshak*. In the criminal context, we seek a search warrant in advance of going to an ISP, Internet Service Provider, for e-mail content. On the civil side, we do not have a policy that has us going to them anyway. We are going to clarify that in our procedures. We think that is currently the case in any event, but, in short, we are following *Warshak*.

Senator GRASSLEY. Well then, I think I can go on to my next subject. Well, maybe one other follow-up. Is the same standard going to be applied to civil and criminal investigations?

Mr. MILLER. My understanding—and you are not talking to a criminal lawyer here—is, we cannot get a search warrant in a civil matter, only in a criminal matter, so we would not be going to the ISP for content of e-mails on the civil side. So it is in conformity with the statute, and it is in conformity with the 6th Circuit opinion in *Warshak*.

Senator GRASSLEY. All right.

Would this apply also to Facebook and Twitter?

Mr. MILLER. You are probably moving out of my range of ability to answer. I will come back to you on that.

Senator GRASSLEY. All right. Well then, why don't you respond to that in writing?

Let me go on to my next and last issue, again to you. You probably know that, a few months ago, I sent a letter to you expressing my concern about the proposed whistle-blower regulations. Chief among these were that they will hamstring the program by limiting awards and discouraging knowledgeable insiders from coming forward.

Last week, the IRS held a hearing on proposed regulations. A number of whistle-blowers and attorneys made their concerns with the proposed regulations loud and clear. If the whistle-blower program is going to be as effective and successful as it can be, the final regulations ought to address those concerns.

Unfortunately, it appears that the concerns expressed by me and others may be falling on deaf ears, because, at last week's IRS hearing, a whistle-blower attorney asked those attending to raise their hands if they thought the proposed regulations would encourage future IRS whistle-blowers to come forward.

It is my understanding that the only persons to raise their hands were the IRS panel members. It is difficult for me to understand how anyone, particularly anyone with knowledge of the concerns expressed by me and others, would not raise their hand.

So do you agree that the IRS panel members are correct, that the proposed regulations will actually encourage whistle-blowers to come forward? I would like to have an explanation of why or why not.

Mr. MILLER. Let me do a few things here, Senator. First—and I hope you know this—I am supportive, and the Service is trying to be more supportive, of the whistle-blower community, with continued contact and discussion with them, of getting information in from them, because there are blind spots for us in reporting. So, in the offshore area and other areas like that, they are vital. We are trying to do what we can. I would say the proposed regulations are just that: they are proposed.

We are talking to people about what changes are necessary, what changes can be made. I think we would also welcome a chance to discuss with you what we can do, what we cannot do, and what might require legislation. So that is sort of where we are.

To the extent we can make whistle-blowers more comfortable and communicate with them more along the way, I think that is a positive. There are a couple of provisions in the administration's 2014 bill that you may know about that are going to help here. One of them will allow us to release more information, I think, to the

whistle-blower towards the end of the process. That also has the detail of requiring them to treat it as 6103 information.

The other piece that you may be aware of and that you have pushed for, Senator, is to have the False Claims Act reprisal rules put into title 26 as well. So I would welcome a conversation, a continued conversation on this, and we are still working on it.

Senator GRASSLEY. I welcome that conversation, because I think it is a situation that is similar to the False Claims Act that you just talked about, which has brought in $33 billion to the Federal Treasury since 1986. I did not anticipate that would ever happen.

I think we have more of a gold mine here if we start listening to these whistle-blowers. I think we have already seen benefits potentially of at least $600 or $700 million, and probably billions of dollars out there that have already been identified. So I will submit some other questions along this line, but I do welcome your talking to me.

I yield the floor.

Senator HATCH. Thank you.

Senator Wyden?

Senator WYDEN. Thank you, Mr. Chairman.

Mr. Miller, on this privacy issue, I want to be clear on it, because this has triggered enormous concern. Are you saying that the agency has not obtained electronic communications without a warrant? That is a "yes" or "no" answer.

Mr. MILLER. I am sorry, you are going to have to repeat that one.

Senator WYDEN. Has the agency obtained electronic communications without a warrant, yes or no?

Mr. MILLER. Not to my knowledge.

Senator WYDEN. All right.

Now, your lawyers say that you can. Mr. Chairman, I would ask unanimous consent to put into the record a memo outlining why the IRS lawyers have taken the view that Americans' e-mail, Facebook messages, and Twitter communications which are older than 180 days can be obtained by the IRS without a warrant.

Senator HATCH. Without objection.

[The information appears in the appendix on p. 109.]

Senator WYDEN. Thank you, Mr. Chairman.

You indicated, Mr. Miller, to Senator Grassley that you would go back and look at this. When will we actually get a public statement that the agency will not seek to obtain electronic communications without a warrant? When would we get that actual public statement?

Mr. MILLER. I think the point I had was that the raising of the issue of Facebook and Twitter—you have that statement from me today, earlier today, Senator Wyden. We are not doing it. What I have said is, in the criminal context, we use search warrants, and we are not going to the ISPs in the civil context for content e-mail, with or without warrant, because we cannot get a warrant in that context in any event.

I will say that there is certain public information out there on Facebook, on Twitter. This is why I sort of want to be more nuanced in the discussion. There is certain public information that we might look at in terms of a collection action, in terms of an examination. That is a different sort of situation, and I would be glad

to come back and sort of work through that for you. But that is public information, not private information.

Senator WYDEN. The public has recently learned, Mr. Miller, that the IRS legal counsel believes that Americans enjoy no general privacy to their online communications that are older than 180 days. That is why people are so troubled. So you have said, and it is certainly helpful to hear that today, that this has not been done in the past. I think it is very important that the agency clarify its policy with respect to the privacy rights of Americans and do it promptly.

Mr. MILLER. And we intend to do that.

Senator WYDEN. When will you do that?

Mr. MILLER. I would hope to have that done—I do not have a date, but it is——

Senator WYDEN. Can you commit today to have this done within 30 days, that the agency will clarify——

Mr. MILLER. I will use my best effort, Senator. I think we can do that, yes.

Senator WYDEN. All right.

Ms. Olson, what is your reaction to this question about the IRS's position with respect to the privacy of tax information? I mean, we are always trying to find ways to boost tax compliance. Here we have—and I put it in the record—the general counsel of the IRS saying that Americans enjoy no general privacy to their online communications that are older than 180 days. That is not something that was made up by some whistle-blower, that was from the IRS general counsel.

My sense is, the two issues are going to be related: taxpayer compliance and the privacy of Americans' tax information. Section 6103 of the Internal Revenue Code was written by the Congress to ensure that taxpayers' tax information is private. What is your sense about memos like this, the one that I just quoted from, undermining the expectation that Americans have in section 6103?

Ms. OLSON. Well, regrettably that memo was not shared with me prior to it being made public, nor was it circulated for my comments. My experience with memos such as that is, when they are actually circulated and people within the IRS, such as my office and myself, have an opportunity to raise concerns about them, that you get a much better quality work product, and it might have looked different had the voice of the taxpayer had an opportunity to comment on that.

I think that it is vitally important to people's willingness to comply with the laws that they feel like they are being treated fairly by the tax administration, just as the tax administration is asking them to behave properly with their tax filing obligations.

Not having a full and robust discussion internally is one sure way of coming out with guidance such as that, so that then it needs to be said, "We are not going to follow that." I just have to say that the Chief Counsel often issues memos in answer to very narrow questions, and, when you have a greater discussion, you are able to place that in context and get a better product.

Senator WYDEN. My time is up, Mr. Chairman. I would just note that, as a general rule, having worked with Ms. Olson over the years, the public is better protected when Ms. Olson is consulted.

I think that we have learned that again, and I hope, Mr. Miller, that that lesson is one of the take-aways of this discussion. Thank you.

Senator HATCH. Thank you, Senator.

Before we turn to Senator Nelson, let me just ask you, Mr. Miller, what are the criminal penalties for a person who commits identity fraud with regard to the IRS; do you know?

Mr. MILLER. I am probably the wrong one to address that question to.

Senator HATCH. Does anybody know there on the panel?

Mr. MILLER. I will say there are two things that are being proposed as part of the 2014 budget that you all should be thinking about. One is, a specific penalty on the civil side of $5,000 for each filing of a false return by reason of identity theft. That would be new. There is also an additional 2-year sentencing guideline that would be brought to bear, or possibly brought to bear. In a tax case where there is an aggregated identity theft rule on the books that does not apply to tax cases, this would put that in.

Senator HATCH. Sure. If you would, I would like to have you folks make recommendations of what type of a criminal penalty there should be for people who engage in these type of practices. I think it ought to be pretty stiff, myself.

Ms. OLSON. Sir, there is, for preparers in particular, a criminal penalty if they use or disclose taxpayer information without the taxpayer's consent. So, when you have a preparer who is using that information to file a return that the taxpayer did not authorize, I think we do have some tools. We have not used that authority, to my knowledge.

Senator HATCH. I am more interested in the actual tax fraud that is being perpetrated.

Senator Nelson, you are next. I apologize for interrupting.

Senator NELSON. First of all, I have been heartened by the commentary that we have heard from the witnesses with regard to either the overall impact of the legislation that we have filed or the parts of it they have testified to.

I would like to pursue just a couple of comments here that will further, I think, give credence to the need for this legislation. I would appreciate, to the chairman and the ranking member, if you all would seriously consider moving this legislation. I think the testimony today has brought out parts of it.

I want to thank Mr. Miller. For example, for some reason we have seen a concentration of this fraud in Tampa and Miami. Senator Isakson came in. There has been a concentration in Georgia as well as Florida, of taking identities and filing false returns and getting a refund. This has such an impact, and we have had a hearing before in this committee a couple of years ago. I just recently had another hearing in my capacity as chairman of the Aging Committee.

What happened in Tampa is that street crime has suddenly dropped because the criminals are using a laptop instead of a crowbar. The drug traffic on the corners has diminished because they found a new way that is a lot easier and a lot less risky to get somebody's money. In this case, it is the United States taxpayers' money.

Mr. Miller, you said you had spent something like $330 million going after ID theft, but you said you had prevented $20 billion of theft. That is a pretty good return on your investment. At the same time, there is still, according to your figures, $5.2 billion that is lost to the taxpayer. So I would be curious, Mr. Miller. Why do you think it is happening in concentrated places like Tampa and Miami?

Mr. MILLER. I do not know that, but where it seems to work, people begin to use it. We really have not gotten behind that. We really do not understand why. It did, in fact—Florida was the beginning of this. You are absolutely right: you still are suffering the greatest amount of this in those two areas.

Senator NELSON. Well, I want to thank you. Working real-time with the local police—here is a good example of government working. They cannot share information. That is prohibited. But we worked it out where, with the victim, the taxpayer giving their consent, that they, the IRS, could share the tax information with the local law enforcement so that it would help them bolster their ability to go after the bad guy.

Now, another way, Mr. Chairman, that they get around this is that they have the tax return money come to a pre-paid debit card, and then there is no identifying information so that the police can go after the bad guy. What do you think about that, Mr. Miller?

Mr. MILLER. I do very much appreciate your comments on our improved work with local law enforcement. We did not start out doing as good a job as we needed to there, and, with your help and the help of Florida authorities, I think we are doing much better.

On debit cards, they were proliferating. I am not sure where they are today. There have been some changes in the rules about, know your customer and the application of those rules to debit cards. We may see a different result now than we did earlier, but it is something we should be talking about.

Senator NELSON. Well, each one of the people, including Ms. LaCanfora from Social Security, has pointed out the problems. Now, they are constrained because they can only do so much with Social Security numbers. But we know it is a problem on the Death Master File. We need to delay the publication.

As she said, the Commissioner of Social Security can go in and make available to legitimate interests, like life insurance companies, the Social Security numbers, but stop publishing them on the Internet. Otherwise, it is like shooting fish in a barrel. If you have the number, somebody is going to go and file a false return. So, Mr. Chairman, with the utmost of urgency on the day after tax day, I would urge you and Senator Hatch to get this legislation moving.

Thank you.

Senator HATCH. Would the Senator yield?

Senator NELSON. Of course.

Senator HATCH. I would like to be on his bill with him. We understand there is an *Ancestry.com* problem that we need to resolve. If we can resolve that, I think I would go on the bill with you.

Senator NELSON. Of course.

Senator HATCH. And I would like to support it and push it.

Senator NELSON. And it is legitimate users.

Senator HATCH. But you only add 2 years' criminal penalty on to the current penalty. Do you know what the current penalty is?

Senator NELSON. Oh yes, sir. The current penalty is only 3 years. The bill takes it up to 5 years. The current fine is only $100,000. The bill takes it up to $250,000.

Senator HATCH. Well, I think the criminal penalties ought to be higher than that so that people realize there is a substantial penalty for doing this type of stuff to their fellow citizens. I just want to commend the Senator for working on this. I would like to be on it. Let us work out that *Ancestry.com* thing so that it works, and I will be happy to work with you.

Senator NELSON. Of course.

The CHAIRMAN. Thank you, Senator.

Senator NELSON. Thank you.

The CHAIRMAN. Senator Cardin?

Senator CARDIN. Thank you, Mr. Chairman. I thank our witnesses.

On a regular basis, I talk to my staff people who handle case work to see what they are spending most of their time on. Identity theft is a major issue in my Senate office, and I would say probably in every Senate office. It is a growing problem. The number of people affected by identity theft, including the IRS issues that we are talking about today, is increasing, and the cases are becoming more complicated.

People are waiting to get refunds who thought their refunds would come in, and it is taking a longer time. The number of people who have been compromised is increasing. So, Senator Nelson, I want to thank you for your leadership on this. I am proud to be a co-sponsor of your bill. You deal with some of the core issues to prevent identity theft, and the careless use of Social Security numbers as an identifier clearly has to change.

I am reminded that, today, I believe the instruction from the IRS is to put your Social Security number on your check, on your returns. I do not know why you need that. That check, after it is—who knows where it is going to be seen or used? It just adds another area of abuse. So I would just urge us to follow Senator Nelson's leadership to minimize the use of the Social Security number much more than we use it today.

I also applaud Senator Nelson for recognizing that we have to work together, the local law enforcement with IRS and Federal authorities, in a much more efficient way to deal with this issue. Our number-one objective is to prevent identity theft. Obviously, once it has occurred, our responsibility is to make sure that those who have been victimized are treated fairly, including getting access to their refunds in a timely way.

As Senator Hatch has pointed out, those who have committed the crime need to be held accountable for their actions so they understand that we will not tolerate this type of crime, which I believe is the fastest-growing crime in America today.

So let me ask, particularly Mr. Miller and Ms. Olson, a question. Any one of you can respond. Basically, what resources do we need in order to accomplish this objective? We talk about tight budgets. What do we need?

A second issue I hope you would address is that we all are very proud that refunds are sent very promptly by the IRS to those who have refunds due. But if it is sent to the wrong person, you are not helping that individual at all. Should we be considering greater audit or greater scrutiny of a tax return as to where the checks are being mailed, or I guess where they are being transmitted, to make sure that we—is there something we can do that maybe will delay the refunds by a day or two, or three or four, but cut down the number of checks that are being sent to wrong accounts on a fraudulent basis?

Mr. MILLER. So let me start in the response. In particular, I will start with the budget. Thank you for asking the question, sir. The IRS, in the last 2 years, is down about $1 billion, 8 to 10 percent, including the $600-million cut we took in sequestration. As I mentioned, we are spending about $330 million in identity theft at this point. It is clear we do need more resources. We need technology dollars, and we need additional employee dollars as well.

The 2014 budget that has come up here has both. It has $100 million for identity theft and 800 FTE, full time equivalencies, as well as some other dollars in the IT area. That is a start. It is not by any means, as you can tell, a full reimbursement of what we are doing, but that is a start. We do need resources, there is no question about it.

Again, I have said this before. I would say if you had a dollar to give me and there was a choice between giving that dollar for an employee or giving it to me for IT improvements, I would take it for IT improvements because, ultimately, that is what we need here, to be better at processing these returns, at matching the information.

Moving to your second area on refund speed, I think it is a discussion we should have. We should have that, whether it is the ability to get W–2s earlier, 1099s earlier, which we are trying to do, but let us face facts. The answer here is that the IRS has as much information as we possibly can at the time we make the decision about issuing a refund. So, I think there are discussion points we ought to have around that.

We also should have discussion points around the other issue you raise, which is, whether it is a debit card or whether it is a direct deposit, there are currently rules elsewhere as to what level of diligence needs to be had between those making the payment into that account and those maintaining the account as to the identity, and do those identities match. That is a discussion that I would welcome, but it is not an IRS discussion. It is not what we regulate. But that is an area fertile for discussion.

Ms. OLSON. If I may. I am aware of the time, but if I may make some comments here. I do believe I named the funding of the IRS a most serious problem for taxpayers, and I think, on the taxpayer service side, which is where identity theft falls, that we are very much suffering. I do believe that there is a lot that can be done with the internal procedures right now that would improve service to the taxpayers.

I think that the larger discussion is this whole refund culture. We have started sort of raising that as an issue. Many other tax administrations in the world actually do not issue refunds until the

filing season is over and they have an opportunity to compare the data that they get in with the returns that they are getting.

That does not just go to identity theft, but all sorts of just mere errors on the returns that they have an opportunity to correct, and then they issue the refunds a month after the filing season is over. I think that is part of the serious discussion we need to have.

With respect to validating the accounts, it used to be 15 years ago that the IRS would get bank information, and the banks would actually verify whether the name on the account matched the name of the check that it was going into. I think direct deposit sort of made that more difficult.

We have gotten various answers about what banking law permits and what it does not, so I think that is something that would be a good subject of study for this committee and other committees as to whether there is a conflict in the law that would prohibit us from being able to do that kind of verification process.

Senator CARDIN. Thank you, Mr. Chairman.

The CHAIRMAN. Mr. Miller, what are you doing about employee sensitivity training? You know, that example. Clearly it is unacceptable that IRS employees hang up on the Kipp Sailes of the world.

Mr. MILLER. It is. It is. It is no way for us to behave. We have trained people. We do train people. We train our CSRs. In fact, we have trained probably 37,000 folks on how to deal with an identity theft situation and to recognize that it is happening, to be sensitive to the folks on the phone who have been victimized. We are trying. We are trying. I think we do well. There are obviously instances where we fail, and we need to work at getting better at that.

The CHAIRMAN. I mean, it really is not difficult at all. Just, anybody who answers the phone has to keep his or her head screwed on straight and remember that they are there to serve the person calling.

Mr. MILLER. Agreed.

The CHAIRMAN. It is not hard. It is pretty simple. I have staff just in my office who take a lot of telephone calls from a lot of people. I marvel at how well they handle all these telephone calls. Do you take calls yourself?

Mr. MILLER. I do take some calls, yes.

The CHAIRMAN. Why don't you go over and sit in one of those offices for a day so they can watch what a good job you do?

Mr. MILLER. I have sat with CSRs, the people who take the phone calls. It is not an easy job, Senator. It is something that they do very well. But there are going to be instances, unfortunately, with 12,000 to 15,000 people, where you have slip-ups and you have failures, and we have to get after those, there is no question.

The CHAIRMAN. When you hire people, they go through training?

Mr. MILLER. They absolutely do.

The CHAIRMAN. Before they get hired?

Mr. MILLER. Well, not before they get hired.

The CHAIRMAN. I am asking, before they get hired.

Mr. MILLER. Do they get training before they get hired?

The CHAIRMAN. No, no, no, no, no. I am just saying, when people apply, do you look at these qualities in an applicant before you decide whether or not to hire them?

Mr. MILLER. We do try to assess whether they are the type of person who could be on the phone and will keep their cool.

The CHAIRMAN. It is better to hire uppers than downers.

Mr. MILLER. Yes. That is why I will never be on the phone.

The CHAIRMAN. You hire uppers, people who are positive, upbeat, they are going to be good employees and they are more likely to treat taxpayers appropriately than if you hire a downer, who is more likely to treat them inappropriately.

Mr. MILLER. Right.

The CHAIRMAN. So what do you think, Ms. Olson? What can be done to increase more appropriate IRS employee response to taxpayers who are calling in, appropriately upset that someone has stolen their ID, and appropriately upset if the Service is not helping them, if the Service thinks, oh, that is not your problem, it is the Service's problem?

Ms. OLSON. I think that it is very difficult when you receive lots of calls in a day to remember that the taxpayer is a human being and not a widget or a case. I think in my own organization what we try to remind my employees of on a regular basis is just that. And the kind of training that we have been trying to do, both in the domestic violence area, where you are working with victims of domestic violence, and moving into the area of identity theft or even just people in economic extremes, is to make employees understand, even if people are angry with you, that it is not personal and that there are ways of ramping down and dialing down the conversation and the emotions. Saying "you are not a victim" is not one of those ways.

So I really think it goes to the nature of training, and it is not a one-time thing; you have to reinforce that message to your employees. You also have to give them a chance to de-brief and to deal with their own stress, because I cannot emphasize enough how difficult it is to be on the phones and listen to people's cases, and it is very easy to try to steel yourself against that pressure.

So, as a manager, I think constantly of how to keep my own employees' morale up even as I am trying to encourage them to listen to the taxpayer, not take it personally, and be empathetic. I cannot emphasize enough that last word.

The CHAIRMAN. I am sure it helps for employees to rotate so they are not sitting in that same place all the time. I mean, for short periods, go off and do something else and then come back again, get refreshed.

Mr. MILLER. I could not agree more. Our difficulty is the number of people we have on the phone and the level of service we try to apply and get to. It is very difficult.

In a better world, I would be taking people off and letting them work paper to decompress. That is not the world of our filing season right now, sir. We do not have the bodies to be able to do that and provide the level of service that is necessary for the American people during tax filing season. So, in particular, this time period is difficult.

The CHAIRMAN. Do you have any goals, benchmarks, that are quantified as to a certain date you would like to see refund waiting lists shortened, or a certain number of days, and the same with ID theft, get it cut down to a certain number of taxpayers whose iden-

tities are stolen? Are you working down to approaching zero on the last category?

Mr. MILLER. We track virtually everything we do, Senator. We certainly do track the efficiency we have. Our difficulty with identity theft is what we need to do is, I agree, get our cycle time down to what is much more reasonable than it is right now. We are getting there. We are closing, again, more cases than we are getting, and that is pretty key.

The CHAIRMAN. But do you have a number? What is it now? What is the cycle time now?

Mr. MILLER. The cycle time is around 180 days.

The CHAIRMAN. Are you trying to get it down to 120?

Mr. MILLER. I would like to get it down to 90.

The CHAIRMAN. I know you would. But you have to get to 120 before you can get to 90. Do you have a date by which you are going to get to 120, another date when you get to 90, another date when you get to 60, another date when you get down to 30?

Mr. MILLER. I do not think I am going to get to 30. One will always have these cases, unfortunately, I believe.

The CHAIRMAN. I am just asking, do you have standards? I mean, do you have numbers that you are aspiring to?

Mr. MILLER. I am aspiring to 90 days by the end of this calendar year.

The CHAIRMAN. Ninety days at the end of this calendar year?

Mr. MILLER. Yes. But that is aspirational, and it depends on the number of cases we get in.

The CHAIRMAN. All right. Let us do it this way. It is 180 today?

Mr. MILLER. Roughly.

The CHAIRMAN. So you want to cut it in half by the end of the year?

Mr. MILLER. Yes.

The CHAIRMAN. And this is April. So let us do a little midway test the 1st of September to see where you are, and let us know.

Mr. MILLER. All right.

The CHAIRMAN. All right. Thanks.

Senator Thune?

Senator THUNE. Mr. Chairman, thank you. I want to thank Commissioner Miller for the penalty relief that you are providing to filers who have been impacted by storms in the south and the Midwest over the past few days.

I can speak from personal experience. In South Dakota, we have had a lot of people without power in our largest community in our State and a few other places, and a lot of damage from recent storms. So, we appreciate your willingness to work with us. I do not know what that extension is going to be, and we look forward to working with you to try to address as best we can the need that people will have to perhaps have a little bit of additional time to get their returns filed.

Let me, if I might, come back to the issue of fraud and ask this question, because I think there are a lot of Americans who would be surprised to know that the IRS does not currently match W–2 information against information reported on tax returns so as to prevent the identity theft-related fraud.

So I am wondering maybe if you can explain why this is the case and what, if anything, the IRS is doing to fix the problem. My understanding is that using W–2 information before a tax refund is issued is one of the recommendations that has been made by the National Taxpayer Advocate, so why is a match-up not done?

Mr. MILLER. The W–2 comes to Social Security, they do a bit of transcription—and my colleague from Social Security can speak to this—then it comes to us rather quickly. We actually have moved it up, and we are doing some matching, but we are not doing matching as of the 1st of February, which would be when we would first begin to make those decisions on refunds. We are doing it a little later in the year. So we are getting better at it.

There is a discussion in the President's budget about going quarterly for wage information or, in our case, we also have a test going on of some State wage data, and we can use that because that is earlier also. So there are other ways to do this. The fact of not having the W–2s is a function of when they come in to the government, and that is a question of burden on both large and small employers.

Second, when we have to start the filing season, that is a question of how fast people want their refunds. Those are pretty big discussion points that we ought to have as we decide where to go here.

Senator THUNE. Ms. Olson, that was a recommendation from the Taxpayer Advocate. Do you want to add anything to that?

Ms. OLSON. Well, we really think that there needs to be a review of the requirements, the due dates, given 21st-century technology of e-filing and availability of data, and can that be moved up so Social Security and the IRS get the information. We have always wondered why it is that the IRS does not get the information first, and we have proposed a pilot for the IRS, which does its own scrubbing of numbers, to determine if it is as good as Social Security in identifying any errors in the data so we do not need to wait that time.

But I think the real thing is, you have to look at the dates, the due dates, of the start of the filing season and the due dates of the 1099 and W–2 information. How soon can you get a reasonable amount, the bulk of these W–2s in, so that you would have them available to match with the returns?

I think you have to pull in the 1099s on the interest and dividends, because people make little mistakes on that, and it would be great to get them up front rather than dealing with them after the fact for filing. That is more a taxpayer service benefit, but, if you are doing one, you might as well do the other.

Senator THUNE. All right. Thanks.

Ms. LaCanfora, this is a little bit off of this particular subject, but I wanted to just ask this question because I posed this question to your predecessor, or I should say I raised the question, I think, before with the Commissioner. But it has to do with last year's annual report on the financial status of Social Security by the trustees of that program.

We obviously know the challenge that the program faces in the long term, but it indicated that you are going to have the Social Security trust fund exhausted by 2033, and the Disability Insurance trust fund facing bankruptcy by year 2016. So you have the

issue of significant benefit cuts perhaps happening automatically for beneficiaries.

That is why this issue, I think, bears on that other one, and that is why I think it is so concerning, the reports of fraud in the SSDI program. The *Wall Street Journal* had reported on some potentially fraudulent practices on the part of law firms such as Binder and Binder, representing claimants for disability benefits before the Social Security Administration, particularly in the appeals process where administrative law judges adjudicate claims.

I guess I am curious as to what actions the Social Security Administration has taken to address allegations about this law firm and their material representations to the Social Security Administration, and how are you prioritizing the Social Security Administration's program integrity functions within your existing budget to ensure that there is a proper response to fraud claims in the SSDI program.

Ms. LACANFORA. A lot of questions there. First, let me just make one comment about the prior discussion with Ms. Olson about the time it takes us to process wage reports. I just wanted to say that, if an employer files a wage report electronically with the Social Security Administration, we turn that around to the IRS within 24 hours, generally speaking, so there really is no delay. That has improved significantly over the past 10 years. I just wanted to put that out there for the record.

With regard to the Social Security Disability Insurance program, there are a lot of things we could talk about there, probably the subject of a whole series of other hearings. But I will say, with respect to any suspicious or fraudulent activity, we have many mechanisms in place to try to combat fraud. I will mention just a couple.

One is our Cooperative Disability Investigation Units, which are units around the country in which we partner with both the Inspector General and local law enforcement to investigate any allegations of fraud and abuse. We do thorough investigations in collaboration with local law enforcement.

In addition to that, we have the mechanism, of course, of our own Inspector General. Our employees around the country, who deal with benefit applications every day, have the ability to refer any suspicious activity to the Inspector General. We believe that with all of the mechanisms we have in place, the fraud in the program is still extremely low. We put it at less than one-half of 1 percent of all claimants who file benefit claims with us.

Senator THUNE. How about specifically the allegations about this law firm and their material representations to the Social Security Administration?

Ms. LACANFORA. From our perspective, we have not substantiated any harm, abuse, or misuse with respect to that law firm.

Senator THUNE. All right. Well, there has been a significant amount of reporting to the contrary, but I appreciate your looking into it and hope you will continue to stay on top of it. Thank you.

Thank you, Mr. Chairman. Mr. Chairman? There is nobody here. [Laughter.]

All right. Well, I guess this hearing is adjourned. Thanks.

[Whereupon, at 11:35 a.m., the hearing was concluded.]

APPENDIX

Additional Material Submitted for the Record

Hearing Statement of Senator Max Baucus (D-Mont.)
Regarding Solutions to Tax Fraud and Identity Theft

The Czech writer and politician Vaclav Havel once said, "I have preserved my identity, put its credibility to the test and defended my dignity. What good this will bring the world I don't know. But for me it is good."

Our identity represents who we are. It represents our morals, our culture, our sense of worth. It represents — as Havel said — our credibility and our dignity. And when stolen from us, it can have devastating consequences.

Identity theft is a serious problem that is growing at epidemic proportions — especially tax-related identity theft. According to the IRS Taxpayer Advocate, tax-related identity theft jumped more than 650 percent between 2008 and 2012. Last year alone, there were 1.8 million incidents of identity theft and fraudulent refunds.

One of the latest victims is Kipp Saile, a 48 year-old horseback outfitter in Pray, Montana, a tiny town just outside Yellowstone National Park. Like many Montana communities, everyone in Pray knows their neighbors. Doors are left unlocked and the only threat of crime involves the possibility of a bear stealing your catch from the Yellowstone River. It is the last place you would expect to find a case of identity theft.

Yet earlier this year, Kipp was in the process of refinancing his home when he got a call from his tax preparer. There was a serious problem. When the preparer tried to submit Kipp's tax return to complete his refinancing, it was rejected by the IRS. According to IRS records, Kipp had moved more than 2,000 miles to Maryland, taken up a new wife and no longer cared for his children.

In reality, of course, Kipp still lived on his ten acres in Pray with his wife of 11 years, Heidi, and their three children. Someone had stolen Kipp's identity and filed a false tax return using his Social Security number. That is where the nightmare began. Kipp has since been forced to spend every day trying to repair the damage to his name and credit.

Needless to say, it has been a stressful experience. It has cost Kipp many a sleepless night and quite a bit of money. The refinance has been put on hold, costing him an additional $500 a month he would have saved with a lower mortgage.

Instead of helping Kipp clear up this mess, the IRS has made a bad situation even worse. Kipp has been told twice by IRS employees that he wasn't defrauded – the U.S. government was. And at least one IRS employee hung up on Kipp while he was trying to make his case.

It's outrageous. I won't stand for a Montanan, or any American taxpayer, to be treated with that kind of disrespect by an agency that is supposed to serve them.

I'm going to say this very clearly Mr. Miller: Never forget that you and everyone else at the IRS work for Kipp Saile, and all American taxpayers. Your job is to serve them. I certainly hope this was an isolated incident that does not reflect the type of service provided by the IRS.

But there is no excuse for even one rude employee like this, and I intend to find out what you're doing to make sure this type of behavior is not repeated. It's critical that the IRS is ready and equipped to handle cases like Kipp's, because they are increasingly common.

We've all seen the stories in the newspapers and on TV about ID theft. Just last week, *USA Today* highlighted some of the most egregious examples of tax ID fraud, like a case where one address in Michigan was used to file 2,137 tax returns. And there was another case where a single bank account was used to receive 590 direct-deposit refunds from the IRS totaling more than $900,000.

In recent Congressional testimony, the IRS reported they had identified more than 900,000 fraudulent returns and stopped more than $6.5 billion in fraudulent refunds in 2011. But that was only the tip of the iceberg.

The Treasury Inspector General for Tax Administration recently reported that another 1.5 million fraudulent returns went undetected in 2011, potentially allowing $5.2 billion in refunds to be paid. The IG estimated that if tax identity theft were not addressed, it could cost the IRS $21 billion in fraudulent refunds over the next five years.

Enough is enough. It is time to act. Three weeks ago, members of this committee were briefed on tax reform options that included proposals to help combat tax fraud and tax ID theft. Senator Nelson, joined by Senators Cardin, Schumer and Feinstein, introduced comprehensive tax fraud legislation last week.

I am pleased that the Administration has included several significant tax fraud prevention proposals in its fiscal year 2014 budget. This includes limiting access to death records and omitting Social Security numbers on wage statements.

But there is still much more that can be done. We know tax fraudsters have easy access to taxpayers' Social Security numbers through online databases, hospitals and other businesses that store personal information. We need tougher controls on access to private information, but it needs to be done efficiently without adding more paperwork to the process.

We know that fraud is easier to detect when the IRS can match a W-2 filed by an employer to a tax return before issuing a refund. Right now, that is not happening. We need to cut through the red tape and ensure this information gets to the IRS quickly.

We also know that too often it can be the tax return preparers themselves who are the identity thieves. Proper oversight by the IRS can help prevent this. But we still face obstacles.

The IRS was handed a major setback recently when a federal court ruled against their authority to regulate tax return preparers. The case, Loving v. IRS, is ongoing, and I am hopeful that the IRS will succeed on appeal. I will be asking for an update on the status of that case in a moment. We need to consider whether additional legislation is necessary to specifically protect taxpayers from fraudulent preparers.

This committee outlined several ideas recently to re-impose tax preparer regulations. I encourage you to look at those ideas that are part of our tax reform option papers.

I also want to hear today how the IRS is utilizing the tools they already have. *USA Today* recently stated the IRS is "losing the identity theft fight" and criticized the IRS for taking too long to resolve fraud cases.

According to the National Taxpayer Advocate it takes, on average, more than 180 days to close cases. That is unacceptable. The IRS needs to step it up and improve the way it handles tax ID theft once cases are identified.

Victims of ID theft – people like Kipp Saile —are forced to put their lives on hold while their cases languish in red tape.

The IRS needs to speed up prosecution through better communication with federal, state and local law enforcement.

This committee is committed to protecting the American taxpayer. I am hopeful that we will be able to work together to move forward with legislation to stop tax ID theft. We owe that to Kipp Saile and all the victims of identity theft.

###

STATEMENT OF HON. ORRIN G. HATCH, RANKING MEMBER U.S. SENATE COMMITTEE ON FINANCE HEARING OF APRIL 16, 2013 TAX FRAUD AND TAX ID THEFT: MOVING FORWARD WITH SOLUTIONS

WASHINGTON – U.S. Senator Orrin Hatch (R-Utah), Ranking Member of the Senate Finance Committee, delivered the following opening statement at a committee hearing examining effective solutions to address tax fraud and identity theft in the nation:

Each year, the Finance Committee holds a hearing around the end of the tax filing season. In the past, these hearings have provided unique insight into the issues faced by American taxpayers as well as some of the overall problems we have with our nation's tax system.

The subject of this year's hearing is the rapidly-growing crime of tax fraud by identity theft. This is a serious matter that deserves our careful attention.

Two of my colleagues – Senator Nelson and Senator Crapo – should be commended for their efforts in this area. Their subcommittee – the Subcommittee on Fiscal Responsibility and Economic Growth – has held two hearings on this topic over the last two years.

In addition, this was an important topic of discussion at last year's tax-filing season hearing before the full committee.

I share the concerns of many throughout our country regarding tax fraud by identity theft. From 2010 to 2011, the number of these crimes nearly tripled, going from about 440,000 to over 1.1 million.

Two senior members of my Finance Committee staff know this issue very, very well as they have been the victims of tax fraud by identity theft. In both cases, criminals obtained their Social Security numbers, filed fraudulent returns, and collected refunds.

For both staffers, this began a nightmarish scenario in which they had to spend days on the phone and filling out paperwork just to be able to file their own tax return. And, in the end, they have to live with the fact that their Social Security numbers are out there and they can only hope that they aren't used to commit another fraud.

So, I want to thank our four witnesses for coming to talk to us about this troubling issue, and I assure you we are listening very carefully.

When it comes to dealing with tax fraud identity theft, I understand that the IRS has adopted a three-pronged approach.

The first prong is prevention, which means stopping this type of tax fraud from being successful in the first place. Clearly, given the prevalence of this crime, much more work needs to be done in this area.

The second prong is providing taxpayer services for those who have been the victims of identity theft. This is a significant focus of the IRS, but it appears that the agency is falling woefully short in some instances.

For example, an audit by the Treasury Inspector General for Tax Administration sampled 17 different identity theft cases and found that the average time it took for these cases to be resolved was 414 days.

That is simply too long a wait for taxpayers who have been the victims of identity theft. I'm hoping we can discuss ways to cut that wait time down during today's hearing.

The third prong of the IRS's approach is catching and convicting the criminals who have committed these crimes. This is a critically important step. If we can step up enforcement, many would-be criminals would likely decide that it's not worth the risk to commit these crimes.

I am interested in hearing more about the IRS's efforts to follow this three-pronged approach, what successes they've had and what challenges they're still facing. That's why I'm glad that we have the top IRS official, Acting Commissioner Steve Miller, here with us today.

In addition, I want to know what other steps could be taken to prevent these crimes, assist the victims, and improve enforcement. I believe all of our witnesses here today will be able to address some of these questions.

While tax fraud identity theft is the major focus of this hearing, we'll also discuss general issues associated with the tax-filing season.

This year, as with every year, taxpayers face a number of issues and obstacles as they try to file their returns. We need to do better in providing assistance during what can be a very difficult time for many of our citizens.

For example, at last year's hearing, I noted that the IRS's goal of answering 61 percent of taxpayers' service calls was unacceptable. I am glad to see this year that the IRS set a significantly higher goal. That said, I still think more can be done to improve taxpayer service.

I hope we can have a full and informative discussion of these issues during today's hearing. Once again, I want to welcome our witnesses. Mr. Chairman, I look forward to this very important hearing.

###

HEARING BEFORE THE
COMMITTEE ON FINANCE,
U.S. SENATE
ON
TAX FRAUD, TAX ID THEFT AND TAX REFORM:
MOVING FORWARD WITH SOLUTIONS

APRIL 16, 2013

STATEMENT OF

MARIANNA LACANFORA
ACTING DEPUTY COMMISSIONER FOR RETIREMENT AND
DISABILITY POLICY
SOCIAL SECURITY ADMINISTRATION

Statement of Marianna LaCanfora,
Acting Deputy Commissioner
for Retirement and Disability Policy,
Social Security Administration
before the Senate Finance Committee

April 16, 2013

Chairman Baucus, Ranking Member Hatch, and Members of the Committee:

Thank you for inviting me to this important hearing on Tax Fraud, Tax ID Theft, and Tax Reform. I will discuss the death information that we maintain to administer our programs, and our collection, use, and safeguarding of wage information. I am Marianna LaCanfora, the Social Security Administration's (SSA's) Acting Deputy Commissioner for Retirement and Disability Policy.

Let me begin by saying that we agree wholeheartedly that the Federal government must do everything it can to combat fraud and curb improper payments. In addition to discussing death information and wage reporting, I will also describe four legislative proposals in the President's budget that, if enacted, would enhance the Federal government's ability to combat fraud and curb improper payments.

Program Overview

We administer the Old-Age, Survivors, and Disability Insurance (OASDI) program, commonly referred to as "Social Security," which protects insured persons and their families against loss of earnings due to retirement, death, and disability. Workers, their employers, and self-employed persons finance Social Security through payroll taxes. We also administer the Supplemental Security Income program, funded by general revenues, which provides cash assistance to aged, blind, and disabled persons with very limited means.

In addition to administering these programs, we handle lesser-known but critical services that bring millions of people to our field offices or prompt them to call us each year. For example, we help administer the Medicare low-income subsidy program and verify information for other Federal and State programs.

The responsibilities with which we have been entrusted are significant. In fiscal year (FY) 2012, we:

- Paid over $800 billion to almost 65 million beneficiaries and recipients;
- Handled over 56 million transactions on our National 800 Number Network;
- Received over 65 million calls to field offices nationwide;
- Served about 45 million visitors in over 1,200 field offices nationwide;
- Completed over 8 million claims for benefits and 820,000 hearing dispositions;
- Handled almost 25 million changes to beneficiary records;
- Issued about 17 million new and replacement Social Security cards;

- Posted over 245 million wage reports;
- Handled over 15,000 disability cases in Federal District Courts;
- Completed over 443,000 full medical continuing disability reviews (CDR); and
- Completed over 2.6 million non-medical redeterminations of SSI eligibility.

Few government agencies touch as many people as we do. The programs we administer provide a financial safety net for millions of Americans, and many consider them the most successful large-scale Federal programs in our Nation's history. We have demonstrated throughout the years that we are effective stewards of program dollars and administrative resources. Moreover, we take great pride in securing the sensitive data and personal information that we maintain to administer our programs.

Collecting Death Information to Administer Our Programs and the History of the Death Master File

Currently, we administer benefit payments to over 61 million beneficiaries and recipients. We collect death information so that we can timely stop paying beneficiaries who have died and pay benefits to survivors of insured persons. Each year, we receive about 2.5 million reports of death primarily from family members, funeral homes, financial institutions, and States. When we receive information about an individual, we update our records, including the Numident file.[1]

Over time, individuals and entities became aware that we were gathering this high-value information. In 1978, Ronald Perholtz filed a lawsuit against us under the Freedom of Information Act (FOIA) to gain access to the death information in our files. In 1980, we entered into a court-approved consent decree that required—and still requires—the agency to release to Mr. Perholtz death information maintained by the agency. The Department of Justice advised us that Congress had not provided an exemption to the FOIA or the Privacy Act that would permit us to withhold the data requested by Mr. Perholtz.

In 1983, Congress added subsection (r) to section 205 of the Social Security Act to require us to collect death information from States to update our program records. This subsection also describes the circumstances under which certain government agencies may receive such information from us. In addition, it specifies that the death information we receive from States is otherwise exempt from disclosure under the FOIA and the Privacy Act. However, the 1983 amendment did not exempt from disclosure death information that we obtain from sources other than the States.

Following the consent decree in the Perholtz litigation, we began to receive additional requests for the same death information that we were providing to Mr. Perholtz. Because we had no legal basis to withhold that death information, we created a file that we could make available to requesters. The file—now commonly known as the public Death Master File (DMF)—contains the non-State death information we maintain to administer our programs.

[1] The Numident contains identifying information associated with a Social Security Number, including a death indicator and parents' names.

Since 1992, due to the growing number of individuals and entities seeking the DMF, we have provided the file to the Department of Commerce's National Technical Information Service (NTIS) to distribute. We chose NTIS because it functions as a national clearinghouse for a wide array of Government data. NTIS's customers include life insurance companies, State agencies, schools, researchers, genealogical services, and financial institutions that, like us, need death information to stop paying benefits to deceased individuals and pay benefits to survivors of insured persons.

Over the years, we have made use of technology to more efficiently administer our programs, including the timely and accurate collection of death information. Since 2002, we have worked with States to increase the use of Electronic Death Registration (EDR). EDR automates our receipt of death information and is highly accurate because the States first verify the name and Social Security Number of deceased individuals against our records before they issue a death certificate or actually transmit the death report to us. Currently 32 states, the City of New York, and the District of Columbia participate in EDR. The death information we collect through EDR is State information, which we do not disclose to the public. (The President's FY 2014 Budget includes an increase of $22 million in Public Health Service Evaluation transfers for the Vital Statistics System supported within the Centers for Disease Control and Prevention (CDC). This increase will allow CDC to gradually phase in electronic death records in the 21 remaining jurisdictions over four years.)

Today, under section 205(r), we provide an electronic file to Federal benefit-paying agencies containing all of our death information on a regular basis, including the death information we receive from the States. The Centers for Medicare & Medicaid Services, the Department of Defense, and IRS are among the many agencies that receive this data. In addition, we provide death information to State agencies administering federally-funded programs. Like us, these benefit paying agencies need death information to ensure accuracy of their benefit payments and prevent fraud, waste, and abuse. In addition, we send certain agencies, including the IRS, a weekly update to the electronic file of all of our death records.

Legislation to Limit Access to Death Information and to Use Death Information to Combat Fraud and Curb Improper Payments

Just as access to accurate death information helps agencies to combat fraud and reduce improper payments, we understand that the public availability of death information could contribute to fraud perpetrated by criminals. We believe that this information should no longer be accessible to those entities or individuals who might misuse it. At the same time, we are mindful that many institutions, such as financial institutions, legitimately need our publicly available death information to combat private sector fraud. As I said earlier, we currently do not have a legal basis to withhold non-State death information under FOIA. Even if we could withhold death information, FOIA does not allow us to withhold death information from certain entities while making it available to others who legitimately need it. Only Congress can strike the proper balance between restricting access to death information and making it available to those entities that legitimately need the information to combat fraud.

Over the past year we have worked closely with an inter-agency group, led by the Office of Management and Budget, to develop a legislative proposal that would strike that balance. I am

pleased to report that the President's FY 2014 Budget includes a legislative proposal that would restrict access to the public DMF. Specifically, the proposal would delay the release of a deceased individual's information on the public DMF for 3 years after he or she dies. This would significantly reduce the ability of criminals to use death information to commit tax fraud. Only private entities that the Commissioner certifies as having a legitimate need for the information—and sufficient protections in place to safeguard the information—would be permitted to receive the public DMF.

At the same time, our proposal would allow additional Federal agencies to access our death information—including State death information—to combat fraud and curb improper payments. Under our proposal, we would be permitted to share our entire death file with Federal agencies for the purposes of public health or safety, law enforcement, tax administration, health oversight, debt collection, payment certification, disbursement of payments, and for the prevention, identification, or recoupment of improper or erroneous payments. We look forward to working with Congress, the Administration, and other parties to refine this legislation.

Additional Efforts to Combat Fraud

A number of Federal agencies are working individually and cooperatively to help assure that their programs do not create opportunities for fraud. For instance, we support Treasury's new Do Not Pay initiative that will help administrators of federally-funded programs reduce improper payments. The Do Not Pay initiative will provide a one-stop shop that will allow these agencies to check various databases, including death information, to identify ineligible recipients and prevent fraud and errors before making payments or awards.

Additionally, the President's FY 2014 Budget also includes a legislative proposal that would remove some restrictions on our ability to share the information that we maintain on prisoners, and expand the data that correctional facilities are required to provide us to include the prisoner's release date. Under this proposal, our prisoner information would become part of the Do Not Pay program, which would make it available to other agencies to help detect and prevent improper payments in a wide array of government programs.

Wage Reporting

Employers are required to file annual reports of their employees' earnings with us. We use this information to ensure that we properly credit employees with the wages they have earned.

Before the mid-1970s, employers were required to report wage information to IRS and SSA on a quarterly basis. However, legislation enacted in 1976 (P.L. 94-202) changed wage reporting to an annual process. Additionally, that legislation required SSA and IRS to develop a single consolidated annual wage report process. Shortly after enactment of that legislation, SSA undertook the responsibility of collecting all wage information through the W-2, Wage and Tax Statement and timely sending that information to the IRS. In return, IRS collects self-employment income and shares the data with us. We use the individual's name and SSN to record his or her earnings.

Employers that file paper W-2s are required to submit their reports to us by February 28 following the end of the tax year. Employers who file reports electronically have until March 31 to file. We process the wage data, and use it to maintain earnings information on every worker for SSA program purposes. On a daily basis, we provide it to IRS for tax administration purposes.

Over the past 10 years, the number of wage reports ranged from a low of 220 million to a high of almost 250 million. The number of employers making reports ranged from 6.3 to 6.7 million annually. We encourage electronic wage reporting because it is more accurate, and we work with the employer community to educate them on its advantages. More and more employers submit their wage reports electronically; in fact, employers filed about 87 percent of W-2s electronically in Calendar Year 2012 -- up from less than 10 percent in 1999.

Legislative Proposals to Enhance the Wage Reporting Process

The President's FY 2014 Budget includes two proposals that we believe would enhance the wage reporting process while also helping to prevent fraud. One proposal would gradually reduce the electronic wage reporting threshold from 250 to 50 employees. Reducing the threshold to 50 would increase the percentage of electronic filing to approximately 90 percent of all W-2s. This will enable us to take better advantage of automation, reduce the work effort required to process paper forms, reduce errors caused by manual processing, and speed the process of correctly posting wages.

The second proposal would restructure the Federal wage reporting process by requiring employers to report wages quarterly rather than annually. Increasing the frequency and timeliness of wage reporting would enhance our ability to detect fraud and curb improper payments in our programs. We recognize that a return to quarterly reporting may be perceived as imposing a burden on businesses, especially small businesses. The Administration is committed to working with the business community to minimize any burden and alleviate any concerns.

Other Initiatives to Enhance Wage Reporting

In addition to the President's FY 2014 Budget proposals, we have some initiatives underway that will help make the wage reporting process more accurate and efficient, thereby providing us with greater capacity. By redesigning our earnings reporting system we will be able to take greater advantage of automation that will result in improved accuracy and faster processing of the ever-increasing number of electronic wage reports.

Also, we are working to greatly reduce paper wage reports, which are error-prone and expensive to process. In FY 2012, we implemented enhancements to our electronic wage report (EWR) filing tool to make it more user-friendly for small business. And the number of registered EWR users has increased from 500,000 in tax year 2009 to over 734,000 in tax year 2012. Through a variety of marketing tools and outreach, we encourage employers to file electronic W-2s through our *Business Services Online.*

Conclusion

We appreciate Congress' interest in working with us to protect our fellow Americans. We are committed to continuing to share death information with our Federal partners and appreciate that there are other parties that, with vigilant oversight, have reasonable and responsible purposes for obtaining death data. We stand ready to assist Congress and the Administration to take steps to combat fraud and improve wage reporting.

WRITTEN TESTIMONY OF
STEVEN T. MILLER
ACTING COMMISSIONER
INTERNAL REVENUE SERVICE
BEFORE THE
SENATE FINANCE COMMITTEE
ON TAX FRAUD AND TAX IDENTITY THEFT: MOVING FORWARD WITH SOLUTIONS
APRIL 16, 2013

INTRODUCTION AND SUMMARY

Chairman Baucus, Ranking Member Hatch and members of the Committee, thank you for the opportunity to update you on the actions we are taking at the IRS to combat refund fraud and help victims of identity theft.

Refund fraud caused by identity theft is one of the biggest challenges facing the IRS today, and the harm it inflicts on innocent taxpayers is a problem we take very seriously. The IRS has a comprehensive identity theft strategy focusing on preventing refund fraud, investigating these crimes and assisting taxpayers victimized by identity theft.

The agency's work on identity theft and refund fraud continues to grow, touching nearly every part of the organization. For the 2013 filing season, the IRS has expanded these efforts to better protect taxpayers and help victims. More than 3,000 IRS employees are currently working on identity theft – more than double the number at the start of the previous filing season. We have also trained 35,000 employees who work with taxpayers to recognize identity theft and help victims. Since the beginning of 2013, the IRS has worked with victims to resolve more than 200,000 cases.

Our fraud detection efforts have increased as well. We expanded the number and quality of our identity theft screening filters, and we have suspended or rejected more than 2 million suspicious returns so far this filing season. The number of identity theft investigations by our Criminal Investigation (CI) division continues to rise, with more than 800 investigations opened so far this fiscal year. A more detailed description of all of our initiatives can be found later in the testimony.

Barriers to further progress do exist, however. One is the sheer volume and complexity of these crimes, as identity thieves continue creating new ways of stealing personal information and using it for their gain. Another is the need to further upgrade our technology in order to implement improvements such as more sophisticated filters and better taxpayer authentication procedures.

Yet another barrier to further progress is the difficult budget environment. The work we are already doing on refund fraud and identity theft involves a difficult balance of resources and staffing at a time when our budget has been reduced by $1 billion over the last two years. We will continue to dedicate staff to resolving identity theft cases,

even at the cost of having fewer people on our toll-free taxpayer service line or on our automated collection program that help us collect past due taxes.

As I describe for you in greater detail our efforts to combat fraud, I urge you to remember that the improvements the IRS is making would not be possible without the additional resources we have directed toward these programs. Even in this challenging budget environment, we have substantially increased our resources devoted to both preventing fraud and serving victims. The IRS spent roughly $328 million on refund fraud and identity theft efforts in FY 2012.

The Administration's Fiscal Year (FY) 2014 Budget request provides $101 million to support IRS efforts to prevent identity theft-related refund fraud, protect taxpayers' identities, and assist victims of identity theft, and enhance the revenue protection strategy implemented in FY 2013. The funding level proposed will permit the hiring of more than 800 additional full-time employees dedicated to identity theft work. The administration's budget request also provides $18.3 million to support continued implementation of the Return Preparer Program, the goal of which is to increase competency levels of tax return preparers. This program complements the IRS' efforts on refund fraud and identity theft, given that these crimes often involve individuals who prepare tax returns on behalf of others to obtain fraudulent refunds.

The budget request also includes several important proposals needed to help us improve our efforts to stop refund fraud caused by identity theft. The Administration proposes to:

- Expand IRS access to information in the National Directory of New Hires for general tax administration purposes, including data matching and verification of taxpayer claims during processing;
- Restrict access to the Death Master File (DMF) to those users who legitimately need the information for fraud prevention purposes and to delay the release of the DMF for three years to all other users. This change would make it more difficult for identity thieves to obtain identifying information of deceased persons in order to file fraudulent returns;
- Grant the IRS the authority to require or permit truncated social security numbers on W-2 forms that employers send to employees, to reduce the risk that the information could be stolen from a paper payee statement by identity thieves;
- Add a $5,000 civil penalty to the Internal Revenue Code for tax-related identity theft; and
- Add the tax-related offenses in Title 18 and the criminal tax offenses in Title 26 to the list of predicate offenses contained in the Aggravated Identity Theft Statute under federal law.

STOPPING THE REFUND AT THE DOOR – ENHANCED RETURN PROCESSING

During FY 2012, the IRS protected $20 billion of fraudulent refunds, including those related to identity theft, compared with $14 billion in 2011. The IRS stopped 5 million suspicious returns in 2012 – up from 3 million suspicious returns stopped in 2011. Of the 2 million suspicious returns suspended or rejected so far this filing season, more than 400,000 were rejected at the point of filing, even before they entered IRS processing systems. The remaining returns generally require further review to determine whether the filer is legitimate. Because these returns require time to review, most are still in open inventory at this time. To date, we have stopped more than 350,000 refunds determined to be fraudulent, worth more than $2.5 billion. The IRS is committed to improving its multi-faceted approach to blocking these fraudulent refund claims, and we strive to operate in such a way that false returns are screened out at the earliest possible stage.

The IRS screens returns for fraud at multiple stages in the processing life-cycle. In 2008, we began placing an indicator on the accounts of taxpayers who have experienced identity theft. These indicators initially served two primary purposes: to speed up account reconciliation for the legitimate taxpayer, and to reduce the likelihood that a taxpayer's information could be used for a fraudulent refund claim in subsequent years. As our identity theft indicator program has developed, we have leveraged it to put in place additional proactive tools that identify fraudulent returns at the point of filing.

In 2011, we launched a pilot program to test the Identity Protection Personal Identification Number (IP PIN). The IP PIN is a unique identifier that authenticates a return filer as the legitimate taxpayer at the time the return is filed. For filing season 2012, the IRS issued IP PINs to approximately 250,000 taxpayers who had identity theft markers on their tax accounts. We verified the presence of this IP PIN at the time of filing, and rejected returns associated with a taxpayer's account where an IP PIN had been assigned but was missing. For the 2013 filing season, we enhanced our programming to increase efficiency, and expanded the IP PIN program to more than 770,000 taxpayers.

Over the last two fiscal years we have made numerous improvements in catching fraud before refunds are issued:

- We implemented new identity theft screening filters to improve our ability to spot false returns before we process them and issue refunds. For example, we designed and launched new filters that flag returns if certain characteristics are detected. While the development of effective filters is complex given the dynamic lives of legitimate taxpayers, these filters enable us to identify fraudulent returns even where a taxpayer's information has not been previously used for filing by an identity thief. These new filters specific to identity theft built on our overall refund fraud detection program, which already identified a significant number of identity theft cases besides those identified by the new filters. We have added even more identity theft filters for the 2013 filing season, including filters that target multiple refunds into a single bank account or to a single address.

- We have accelerated the use of information returns in order to identify mismatches earlier. Moving this matching process forward in time has enhanced our ability to identify fraudulent tax returns before we process them. We are accelerating more types of information return data in 2013.

- We have implemented a variety of mechanisms to stop the growing use by criminals of deceased individuals' identity information to perpetrate fraud. Once we confirm the fraud, we lock the accounts of these individuals so that no further misuse will occur. We also routinely lock accounts of deceased taxpayers once they no longer have a filing requirement. To date, we have locked more than 9 million accounts. As noted above, the Administration is proposing a legislative change to the practice of routine release of the Death Master File.

- We have developed procedures for handling information about identity theft victims received from law enforcement officials, who discover this information in the course of investigating identity theft schemes or other criminal activity. This data is extremely valuable. It can be used to flag taxpayer accounts and help us block returns filed by identity thieves who attempt to use the personal information of those taxpayers to file a fraudulent return. Our Criminal Investigation (CI) Division will use this data to identify links between criminal schemes, and will share this information when appropriate to ensure that victims' accounts are adjusted and protected from future identity fraud.

- We expanded the use of our list of prisoners to better stop the processing of problematic returns. In FY 2012, we stopped over 220,000 fraudulent returns filed by prisoners. This represents over $2.5 billion in refunds stopped, a more than 10 percent increase over FY 2011. The IRS has collaborated with the Bureau of Prisons and states that choose to partner with us to help identify prisoners who may be engaged in tax fraud, and we received additional help in 2011 with the passage of the United States-Korea Free Trade Agreement Implementation Act, which included language requiring federal and state prisons to provide information on the current prison population. Although the authority allowing us to share return information with prisons expired at the end of 2011, it was renewed and made permanent in the American Taxpayer Relief Act enacted earlier this year. In addition, the Social Security Administration is proposing reforms to use its prisoner data that will further help IRS reduce improper payments.

- We are collaborating with software developers, banks, and other industries to determine how we can better partner to address identity theft and prevent federal monies from reaching the hands of identity thieves. For example, we established a cooperative agreement with more than 100 financial institutions to reject questionable deposits. The IRS also established relationships with representatives of the prepaid access card industry, which has security protocols designed to detect and prevent fraudulent use of the cards. In many cases,

these companies may have the ability to identify potentially fraudulent tax refunds and freeze or cancel the cards.

The IRS will continue to strengthen our efforts to catch identity theft and other fraud before erroneous refunds are issued. We will continue refining our filters aimed at detecting and preventing the processing of fraudulent returns, and develop new methodologies as needed. Additionally, we are considering new technologies for authenticating the identities of taxpayers at the time of filing as a future means of precluding tax-related identity theft.

ASSISTING TAXPAYERS

Improving our Processes

The IRS understands that identity theft is a frustrating, complex process for victims. While identity thieves steal information from sources outside the tax system, the IRS is often the first to inform a victim that identity theft has occurred. We realize the importance of resolving cases involving identity theft quickly and efficiently, allowing taxpayers victimized by identity theft to receive their refunds as soon as possible and preventing adverse enforcement actions from being taken against them. To that end, we continue to develop and implement new procedures to improve the service provided to identity theft victims.

During FY 2012, the IRS reengineered our identity theft process to close cases more efficiently and accurately and to find ways to reduce customer burden. As a result, we have made a number of programming and procedural enhancements, enabling us to move faster to identify accounts with a high potential for identity theft. Cases generated as a result are reassigned for review more quickly than in the past. Other procedural enhancements are helping us to reduce delays in releasing refunds to the legitimate filer in cases where duplicate returns are filed.

In the first three months of 2013, the IRS worked with victims to resolve and close more than 200,000 cases. This is in addition to the expansion of the IP PIN program mentioned above. The IRS has dedicated more employees to resolve victim cases. These are extremely complex cases to resolve, frequently touching on multiple issues and multiple tax years. Cases of resolving identity can be complicated by the thieves themselves calling in. The IRS is working hard to streamline its internal processes, but much more work remains. A typical case can take about 180 days to resolve; however, we are actively working to reduce this inventory to shorten that time period.

We are also continually improving the way we track and report on the status of identity theft cases, which we believe will lead to quicker case resolution and provide innocent taxpayers with the most current account information and status of their refunds. Additionally, better tracking and reporting means that we can spot – and correct – any flaws in the system more quickly.

Employee Training

The IRS runs one of the largest phone centers in the world, and we are dedicated to providing quality service with a high degree of accuracy to every taxpayer who contacts us. We realize, however, that taxpayers who contact us with identity theft problems present unique challenges to our telephone representatives, and we are committed to providing our assistors with the information they need to ensure these taxpayers receive quality, courteous service. As part of this effort, we conducted a thorough review in 2011 of the training we provide our employees to make sure that they have the tools they need to respond appropriately to those who have been victimized by identity theft.

As a result of this review, we provided our telephone assistors with updated training this past filing season to ensure they better understand the serious financial problems of identity theft victims and maintain the proper level of sensitivity when speaking with victims. Additionally, we broadened the scope of our training beyond telephone assistors to cover all IRS employees who might interact with identity theft victims. We developed a new training course that includes sensitivity training as well as training on the proper tools and techniques to use when handling identity theft cases. In all, 35,000 IRS employees have received this training.

Taxpayer Outreach and Education

The IRS continues to undertake outreach initiatives to provide taxpayers, return preparers, and other stakeholders with the information they need to prevent tax-related identity theft and, when identity theft does occur, to resolve issues as quickly and efficiently as possible. As part of our outreach efforts, we overhauled and updated the identity protection training provided to tax practitioners at our annual Nationwide Tax Forums in 2011 and again in 2012. These annual events, held in several cities around the country, draw more than 16,000 practitioners, who attend to learn about key tax laws and issues. In addition, we met with practitioners to discuss the IP PIN program, the expansion of the program, and the modified procedures, forms, and notices associated with the program. We are also working closely with software developers to ensure that instructions regarding the use of an IP PIN are included in their products.

We have a far-reaching communications effort that uses both traditional and social media channels to relay information on identity protection issues. As part of this effort, we have produced new identity theft awareness videos for the IRS YouTube channel in English, Spanish, and American Sign Language, and we distributed identity protection information through IRS Twitter feeds and podcasts. We continue to update the identity theft information provided on the IRS.gov website. This includes emerging trends in identity theft along with fraud schemes, phishing sites, and prevention strategies. We also added a direct link to our Identity Theft page, to make it easier for taxpayers who visit IRS.gov to locate this information. We have issued a number of news releases and tax tips to help taxpayers and to highlight our continuing enforcement efforts. We plan

to continue this sweeping communication effort in the upcoming filing season and beyond.

CRIMINAL INVESTIGATION WORK

The investigative work done by CI is a major component of our efforts to combat tax-related identity theft. CI investigates and detects tax and other financial fraud, including fraud related to identity theft, and coordinates with other IRS divisions to ensure that false refunds involving identity theft are addressed quickly and that the IRS accounts of identity theft victims are marked to help prevent future problems. CI recommends prosecution of refund fraud cases, including cases involving identity theft, to the Department of Justice.

In response to the growing threat that identity theft poses to tax administration, IRS established the Identity Theft Clearinghouse (ITC), a specialized unit within CI that became operational in 2012, to work on identity theft leads. The ITC receives all refund fraud-related identity theft leads from CI field offices. The ITC's primary responsibility is to develop and refer identity theft schemes to the field offices, facilitate discussions between field offices with multi-jurisdictional issues, and provide support to ongoing criminal investigations involving identity theft.

Investigations of tax fraud related to identity theft have increased significantly over the past three fiscal years. In FY 2012, CI initiated 900 investigations involving identity theft, which is more than triple the number of investigations in FY 2011. Indictments in identity-theft related cases also increased significantly, totaling nearly 500 in FY 2012, with 223 individuals sentenced and an average time to be served of 48 months. This compares with 165 indictments, 80 individuals sentenced, and a 44-month average sentence in FY 2011. Additionally, the direct investigative time spent by CI on identity theft cases has increased by 129 percent in FY 2012 over FY 2011.

This trend is continuing in FY 2013. Already through April 9, 2013, more than 800 criminal identity theft investigations have been opened. Indictments in identity theft-related cases total 607, with 197 individuals sentenced and an average time to be served of 44 months.

In collaboration with the Department of Justice's Tax Division (DOJ-Tax) and local U.S. Attorneys' offices, the IRS conducted a highly successful coordinated identity theft enforcement sweep in January 2013. This nationwide effort against 389 identity theft suspects led to 734 enforcement actions, including 189 indictments, informations and complaints, and 109 arrests. Around the time of the sweep, IRS auditors and investigators conducted compliance visits to 197 money service businesses in a variety of locations across the country to help ensure that these businesses were not facilitating refund fraud and identity theft.

Our collaborative efforts extend to other federal agencies as well. For example, the IRS has worked with the U.S. Postal Inspection Service (Postal) to provide training updates on how to handle refund checks and prepaid access cards diverted as part of Postal's fraud detection process. We also issued updated guidance to other federal law enforcement agencies, including the Secret Service and the Federal Bureau of Investigation, on available methods for returning stolen refund amounts to the Department of the Treasury.

The IRS continues to seek out additional methods to combat the proliferation of tax-related identity theft. In July 2012, the IRS expanded the number of charges that special agents investigate when identity theft matters arise in the context of fraudulent returns. The additional charges include: Forging Endorsements on Treasury Checks; Theft of Public Money; Fraud in Connection with Access Devices; Mail Fraud; and Wire Fraud.

Aiding in the fight against identity theft, in September 2012, DOJ-Tax issued Directive 144, Stolen Identity Refund Fraud (SIRF), to provide federal law enforcement officials with the ability to timely address a subset of identity theft cases. This directive specifically focuses on identity theft in the context of fraudulent tax refunds and provides for streamlined initiation of these investigations and prosecutions. CI subsequently responded by streamlining investigative and review processes to capitalize on these historic changes and will continue to move expeditiously on SIRF investigations.

State and local law enforcement agencies also play a critical role in fighting identity theft. CI regularly collaborates with these agencies, and this effort will only increase in the future. Over the past several years, CI has established or participated in at least 35 task forces and working groups around the country in an effort to leverage the resources and expertise of various law enforcement agencies to address identity theft-related crimes.

The IRS also has been working to assist state and local law enforcement agencies in the efforts they are making to fight identity theft-related refund fraud. One way we have done this is by developing the Identity Theft Victim Disclosure Waiver Process, which was launched in Florida in April 2012.

This program provides for the disclosure of federal tax returns and return information associated with the accounts of known and suspected victims of identity theft with the express written consent of those victims. Prior to disclosing any tax information, victims are required to sign a waiver authorizing the release of information to the designated state or local law enforcement official pursuing the investigation. To date the IRS has received more than 1,560 waiver requests from more than 100 state and local law enforcement agencies in the nine states that have been participating in the pilot. On March 28, 2013, the IRS announced that this program has been expanded to all 50 states.

Some of the IRS' recent successes involving identity theft include the following cases in which sentences were handed down over the last several months:

- On April 3, 2013, a Florida man was sentenced to 70 months in prison and three years of supervised release for his participation in a $3.3 million identity theft scheme that resulted in charges of conspiracy to file fraudulent claims and aggravated identity theft. Some of the personal information used by this individual was stolen from a community college's financial aid office.

- On March 22, 2013, a New York man was sentenced to 41 months in prison on charges that included identity theft and impersonating an IRS employee and a New York State Department of Labor official. This individual fraudulently obtained tax refunds by stealing taxpayers' personal information or tricking them into disclosing the information to him.

- On March 18, 2013, a California man was sentenced to 54 months in prison and ordered to pay more than $1.3 million to the IRS in connection with a scheme involving the filing of false tax returns. The individual and his associates used the names and social security numbers of residents of Puerto Rico to file more than 1,000 false returns seeking refunds based on the earned income tax credit. This individual also used false out-of-state driver's licenses to set up private mailboxes to receive the refund checks.

- On March 7, 2013, a Florida man was sentenced to 192 months in prison, three year of supervised release, and ordered to pay more than $100,000 in restitution to the IRS on charges of access device fraud and aggravated identity theft. The individual was found to have in his possession 28 pre-paid debit cards loaded with $117,000 in tax refunds.

- On February 22, 2013, a Florida man was sentenced to 159 months in prison and three years of supervised release on charges of access device fraud and aggravated identity theft. By searching an online database, this individual obtained the social security numbers of more than 23,000 people whose birth dates he had already obtained. He provided this information to associates who filed fraudulent returns.

- On February 8, 2013, an Alabama woman was sentenced to 65 months in prison on charges including aggravated identity theft and fraud in connection with computers. While working at a medical center records office, this individual stole more than 800 names, social security numbers and other personal information from current and former patients, and then sold the information to another person who used the information to file false tax returns.

- On October 1, 2012, two North Carolina men were sentenced to a total of 155 months in prison and ordered to pay a total of $466,153 in restitution for their involvement in an identity theft scheme. The individuals broke into a tax preparation office, stealing over 300 files containing the personal information of tax clients. Using this information, the individuals filed returns in the names of

the clients and directed the tax refunds to either debit cards that were mailed to addresses they controlled or to bank accounts that were opened using fraudulent and unauthorized information.

- On September 21, 2012, an Arizona woman was sentenced to 36 months in prison and ordered to pay $386,938 in restitution on charges related to her involvement in a conspiracy to commit identity theft. The defendant utilized stolen identities to file 180 tax returns to falsely claim more than $1,000,000 in tax refunds. The defendant concealed the fraud by filing the tax returns electronically using the unsecured wireless networks of neighbors, directing the refunds to prepaid debit card accounts obtained using false identities, and recruiting friends and associates to receive the prepaid debit cards by mail at various addresses.

CONCLUSION

Mr. Chairman, thank you again for the opportunity to update you on the steps that the IRS is taking to prevent identity theft and to assist taxpayers who are victims of this crime. Fighting identity theft will be an ongoing battle for the IRS, and one where we will not let up. Our work here is critical. We cannot be lax either in stopping fraud or in assisting taxpayers who have had their identities stolen. Although we cannot stop all identity theft, our efforts thus far have provided a solid foundation upon which we will continue to build and improve. We have to act aggressively because we have a responsibility to preserve the public's faith in the essential fairness and integrity of our tax system. I would be happy to answer any questions that you may have.

Questions for the Record
"Tax Fraud, Tax ID Theft and Tax Reform: Moving Forward With Solutions"
Questions for Steven T. Miller
Hearing Date: April 16, 2013

Questions from Senator Robert P. Casey, Jr.

1. Law enforcement officials in Pennsylvania have been outspoken about the size of the identity theft /tax fraud problem. According to one Pennsylvania District Attorney, tax fraud is the single most profitable crime in his jurisdiction. This problem is exacerbated by his inability to go after these criminals. You have heard these frustrations from others, including other members of this Committee. To address these concerns, the IRS has initiated an information-sharing pilot program. Can you speak to the success of this program to date? Also, what more needs to be done to address the problem? As this Committee looks to work on legislation what can we do to enhance the tools at your disposal?

Response

Success of the Program to date:

ENFORCEMENT – VICTIM WAIVER DISCLOSURE PROGRAM

Overview:

Local law enforcement and other federal agencies play a critical role in combating identity theft. As part of this collaborative effort, the IRS developed the Identity Theft Victim Disclosure Waiver Process, which was launched as a pilot in Florida in April 2012. This program provides for the disclosure of federal tax return information associated with the accounts of known and suspected victims of tax-related identity theft with the express written consent of those victims. Prior to disclosing any tax information, victims must sign a waiver (Form 8821-A) authorizing the release of information to the designated state or local law enforcement official pursuing the investigation.

Based upon increased interest from other areas of the country, the program was expanded to include the States of Alabama, California, Georgia, New Jersey, New York, Oklahoma, Pennsylvania and Texas, in October 2012. At the end of March 2013, the program was expanded to include all 50 states . IRS Criminal Investigation employees in the newly expanded areas are currently involved in a variety of outreach and trainings efforts. Since the program's inception, the IRS has received over 1,950 waivers authorizing the disclosure of returns and related information to 133 participating law enforcement agencies.

Successful Prosecutions:

The following examples highlight some of the successful prosecutions by state and local authorities that have occurred as a direct result of the return information provided in response to this program;

- Demetrius Lewis was arrested by the Florida Department of Law Enforcement (FDLE) in connection with tax-related identity theft activity on September 12, 2012. The matter involved significant press coverage associated with the Identity Theft Victim Disclosure Waiver Process Program in the greater Tampa area. Lewis is currently awaiting trial in connection with 9 counts of identity theft. Upon discovering refund checks were deposited into bank accounts controlled by Lewis, FDLE was the first agency to seek assistance in identifying victims and actively pursued the use of Forms 8821-A to obtain return and return information that was utilized in support of state charges against Lewis.

- Bobby Arrington was one of nineteen individuals arrested by the Polk County Florida Sherriff's Department's Operation Stop the Drop prior to the ID Theft Waiver Disclosure Program being authorized. Forms 8821-A were subsequently used to assist the prosecution. Arrington was charged with 23 counts of identity theft. The investigation revealed that Arrington obtained refunds totaling $7,398 in connection with 8 identity theft returns. Arrington was also sentenced to serve 5 years followed by probation.

- In February 2013, the Manhattan District Attorney's Office sought IRS's assistance with the prosecution of Peter Murmylyuk. Murmylyuk was associated with a tax-related identity theft matter involving over 125 returns and almost $500,000 in lost refunds. Murmylyuk was indicted several months prior to the Identity Theft Victim Disclosure Waiver Process Program being expanded to the State of New York and was originally set for trial on February 25, 2013. As a result the IRS was able to provide the DA's Offices with associated returns and refund payment information. On April 15, Murmylyuk entered a guilty plea and is currently awaiting sentencing, which carries a recommended range of 3 to 9 years.

What more can be done?

The improvements the IRS is making would not be possible without the additional resources we have directed toward these programs. Even in this challenging budget environment, we have substantially increased our resources devoted to both preventing fraud and serving victims.

The Administration's Fiscal Year (FY) 2014 Budget request provides $101 million to support IRS efforts to prevent identity theft-related refund fraud, protect taxpayers' identities, assist victims of identity theft, and enhance the revenue protection strategy implemented in FY 2013. The funding level proposed will permit the hiring of more than 800 additional full-time employees dedicated to identity theft work. The Administration's budget request also provides $18.3 million to deliver high-priority, preparer related enforcement activities to improve taxpayer compliance and ensure the accuracy of returns filed by tax professionals. This program complements the IRS' efforts on refund fraud and identity theft, given that these crimes often involve individuals who prepare tax returns on behalf of others to obtain fraudulent refunds.

In addition, the budget request includes several important proposals needed to help us improve our efforts to stop refund fraud caused by identity theft. The Administration proposes to:

1. Expand IRS access to information in the National Directory of New Hires for general tax administration purposes, including data matching and verification of taxpayer claims during processing;

2. Restrict access to the Death Master File (DMF) to those users who legitimately need the information for fraud prevention purposes and to delay the release of the DMF for three years to all other users. This change would make it more difficult for identity thieves to obtain identifying information of deceased persons in order to file fraudulent returns;

3. Grant the IRS the authority to require or permit truncated social security numbers on W-2 forms that employers send to employees, to reduce the risk that the information could be stolen from a paper payee statement by identity thieves;

4. Add a $5,000 civil penalty to the Internal Revenue Code for tax-related identity theft; and

5. Add the tax-related offenses in Title 18 and the criminal tax offenses in Title 26 to the list of predicate offenses contained in the Aggravated Identity Theft Statute under federal law. A conviction for aggravated identity theft adds two years to the sentence imposed for the underlying felony.

2. The same DA, John Adams from Berks County, PA, recently shared an example. According to the DA, his detectives recently spent about 40 hours investigating a claim. Their efforts led them to an IP address in Canada. At that point, they could do little more than refer the case back to the IRS. It is his feeling that, "this incident again exemplified that we cannot arrest our way out of this problem." In the face of his challenges, his questions are: "What steps are being taken to increase verification of W-2's, identities, IP addresses, and social security numbers to prevent tax fraud from occurring in the first place?"

Response

The IRS is placing a heightened emphasis on the prevention and detection of identity theft and refund fraud on returns submitted to the IRS. We have implemented, and continue to refine, our business processes to improve identification and prevention of tax fraud.

The Electronic Fraud Detection System (EFDS) identifies potential fraudulent returns. This system relies on data mining scores, fraud models and algorithms to determine the likelihood of fraud. As part of this process, we also look for similar attributes or characteristics such as a primary address that has been used multiple times on different returns or an IP address that is consistently used in the filing of fictitious claims.

The IRS uses a process of income verification in its risk assessment of whether a return is fraudulent. We have accelerated the use of information returns (e.g., Forms W-2) in order to

identify mismatches earlier. Moving this matching process forward in time has enhanced our ability to identify fraudulent tax returns before we process them.

In addition to EFDS, the IRS built identity theft screening filters to improve our ability to spot false returns before we process them and issue refunds. For example, we designed and launched new filters that flag clusters of returns if certain characteristics are detected such as multiple refunds into a single bank account or to a single address. While the development of effective filters is complex given the dynamic lives of legitimate taxpayers, these filters enable us to identify fraudulent returns even where a taxpayer's information has not been previously used for filing by an identity thief.

One of our primary strategies to assist past victims of identity theft and prevent further fraudulent filings is the creation of an Identity Protection Personal Identification Number (IP PIN). The IP PIN program began in 2011 and has since been expanded and enhanced to protect victims of identity theft by creating an additional layer of security by requiring the IP PIN when filing a tax return. The IP PIN allows the IRS to more effectively identify fraudulent returns, while at the same time, validate that the return filed is the legitimate taxpayer's return. For the 2013 filing season, we issued more than 770,000 IP PINs and have improved processing of returns filed with an IP PIN. Additionally, the replacement IP PIN process (for taxpayers who lose or misplace their original IP PIN) has been significantly streamlined to provide better service. Taxpayers are asked to validate their identities by answering a series of questions for disclosure level authentication and if validated, they receive the replacement IP PIN at the point of contact.

Beginning in 2008, we implemented the use of identity theft markers which are placed on a taxpayer's account to identify an identity theft incident. These markers are used to distinguish legitimate returns from fraudulent returns and prevent victims from facing the same problems every year. The markers provide additional protection from identity thieves by systemically evaluating taxpayers' future returns to check for inconsistencies and discrepancies that indicate potential fraudulent filing.

We are also attempting to prevent the growing misuse of decedents' social security numbers by detecting and stopping potentially fraudulent returns. We are coding the accounts of deceased taxpayers who were previously victimized and where there is no longer a future filing requirement. This coding "locks" a taxpayer's account, preventing the acceptance of potentially fraudulent returns. In addition, the President's Budget for FY2014 includes a legislative proposal that would restrict immediate access to the list of deceased individuals' SSNs known as the Death Master File (DMF) maintained by the Social Security Administration to those users who legitimately need the information for fraud prevention purposes and would delay the release of the DMF for three years to all other users.

Additionally, the IRS is reducing the use of SSNs on our systems, forms, notices, and letters to protect taxpayers from identity theft. Also, as mentioned in response to question #1, the Administration's FY2014 Budget includes a legislative proposal to grant the IRS authority to require or permit truncated social security numbers on W-2 forms that employers send to employees, to reduce the risk that the information could be stolen from a paper payee statement by identity thieves.

To address tax refund fraud associated specifically with direct deposit to prepaid and other forms of debit and bank accounts, the IRS and Treasury's Financial Management Service (FMS) have collaborated with NACHA, the Electronic Payments Association, to develop an opt-in program for interested financial institutions to enable them to return ACH direct tax refund deposits if they suspect the transfers were based on fraudulent returns. The IRS Refund Return Opt-In Program will help the IRS examine the validity of refunds already issued and stop payment on or recover invalid refunds; build better pre-refund filters; and prevent future fraudulent refunds.

3. St. Luke's is a major healthcare provider in the Lehigh Valley. Recently, they expanded, adding a second location, which was established as a separate entity. St. Luke's submitted a 501(c)(3) application for this location in in February 2012. They are still waiting. Part of the reason for the delay is the 501(r) requirements under the Affordable Care Act, which adds requirements to hospitals applying for 501(c)(3) designations. However, these rules have not been finalized. Given this, why are Pennsylvania hospitals being held to 501(r) requirements in 2013, prior to the full implementation of the Affordable Care Act next year?

Response

Section 9007 of the Affordable Care Act (ACA) added section 501(r) to the Code which imposes additional requirements that hospital organizations must meet in order to be described in Internal Revenue Code section 501(c)(3). With the exception of the Community Health Needs Assessment requirement, these additional requirements apply to taxable years beginning after the date of enactment of the ACA (March 23, 2010). The Community Health Needs Assessment requirement became effective for taxable years beginning after March 23, 2012. The ACA did not otherwise affect the existing substantive standards for tax exemption under section 501(c)(3).

The processing of an application for recognition as a tax-exempt organization often involves the review of complex issues. With regard to the specific organization mentioned in your question, its application for recognition as a 501(c)(3) organization was approved by letter dated April 26, 2013.

Questions from Senator Charles E. Grassley

1. At the hearing I asked you about the IRS's policy in accessing the electronic communication of taxpayers, such as emails. You indicated the IRS adheres to the 6th Circuit's decision in U.S. v. Warshak. However, as was discussed, recent press reports and internal documents indicate otherwise. Please describe current procedures and how they differ from the standards under ECPA, if at all. In addition, please provide any relevant supporting documents, such as internal manuals, that indicate this is in fact IRS's policy.

   Response

   In certain limited circumstances, the IRS will seek to obtain the content of email communications from Internet Service Providers (ISPs) during the course of active criminal investigations. In such cases, the IRS will obtain search warrants with the assistance of the Department of Justice, consistent with all applicable federal laws and regulations. The current policy of the IRS is not to seek the content of email communications from ISPs in civil matters. Policy Statement 4-120 was signed in May 2013, making it clear that the IRS will follow the holding in *United States v. Warshak* in all judicial circuits. This policy statement is available on irs.gov and will also be available in the Internal Revenue Manual. The IRS will continue to review this issue and policies and guidance to update them as necessary.

2. Do the same procedures apply to all forms of electronic communication, including, but not limited to, text messages and private messages sent through social media, such as Facebook and Twitter? If not, please explain the differences and any reasons supporting the different treatment.

   Response

   We are reviewing this issue, including the application of our policies and procedures to different forms of communication through social media, and will update our policies and guidance as appropriate.

3. Are there any circumstances that exist in which the IRS takes the position it can access private electronic communication without a warrant? Please explain.

   Response

   There are specific situations in ongoing examinations or investigations, outside the context of the Electronic Communications Privacy Act and the Stored Communications Act, in which the IRS can and does request the content of emails directly from the author or the recipient of the email communication. For example, in individual examinations, the IRS may request that taxpayers under examination provide their own supporting information, which may include electronic records, such as emails. In addition, IRS examinations sometimes lead to civil litigation. In those circumstances, the federal court discovery rules specifically provide that parties may seek

electronic records. In both situations, the taxpayer is aware of the information request, has all the rights and protections afforded under the law, and may challenge any such request in court.

4. Please explain why, if your policy is the IRS needs a warrant to access private email or electronic communications, the Internal Revenue Service Manual has not been updated and the existence of the 2011 Chief Counsel Memorandum that indicates otherwise.

Response

We are currently in the process of reviewing and updating our guidance.

5. When can the public expect the IRS to update its internal and public manuals to provide clarity for when a taxpayer's electronic communication can be accessed? Once the relevant manuals and material has been updated, will you ensure that copies are provided to me and my staff?

Response

Policy Statement 4-120 was signed in May 2013, making it clear that the IRS will follow the holding in *United States v. Warshak* in all judicial circuits. The policy statement is available on irs.gov and will also be available in the Internal Revenue Manual. The IRS is currently reviewing its policies and guidance to update them to ensure conformity with this policy statement. We will provide you and your staff copies of the relevant Internal Revenue Manual updates.

6. In response to Senator Wyden, you said to the best of your knowledge the IRS has never accessed a taxpayers email without warrant. After conferring with appropriate IRS personnel and reviewing any and all relevant documents, can you confirm the IRS has never accessed any taxpayer's electronic communication without a warrant? Please indicate in how many instances, if any, that the IRS obtained electronic communication without a warrant.

Response

IRS senior executive leadership recently learned of a few instances in which the IRS sought to obtain the content of email communications from an ISP by issuing a civil summons. Those summonses were withdrawn.

7. You indicated at the hearing that the IRS will look at social media profiles, such as Facebook and Twitter, because you take the view that the profiles are public, not private. Please explain what sort of standard exists before the IRS will start combing these sites to dig up information on a taxpayer? What, if any, limit exists?

Response

The IRS does not select taxpayers for examination based on searches of social media sites. Taxpayers are selected for examination based on the information contained on the individuals' tax returns and, in some instances, through information we receive from third parties. The IRS is considering what limitations, if any, should be placed on the use of publicly available social media information in an ongoing examination or collection action. If we adopt new internal procedures, we would make them public. The IRS is not considering the use of non-public information (such as private online social media profiles) in these actions.

8. A concern I hear from whistleblowers over and over again is that there is a lack of communication from the IRS. At the hearing you indicated the IRS is trying to be more supportive of whistleblowers through continued contact and communication. Could you please provide examples of recent steps that have been taken to increase contact and communication with whistleblowers?

Response

Presently, the IRS has no authority under section 6103 to respond to requests for the status of IRS action, or for information about the scope of issues being addressed in an audit. The President's Budget for FY2014 includes a legislative proposal that would extend existing criminal sanctions for improper disclosure of taxpayer information to include disclosures by whistleblowers and their representatives of information provided to them as part of an award determination administrative proceeding. Congressional consideration of this proposal would provide an opportunity to address the merits of expanding the scope of permissible disclosures and the balance between whistleblower and taxpayer interests.

In an effort to increase communication with whistleblowers, in the proposed regulations issued for comment on December 18, 2012, there is a proposal to provide additional communications after an examination is complete and proceeds are collected. In cases where an award may be payable under 7623(b), the award determination administrative proceeding would start at the point when there are collected proceeds from which an award may be payable. In cases where an award is not payable under 7623(b), or where a payment will be made under 7623(a), a limited administrative proceeding would permit the Whistleblower Office to provide some information about the reason for denying the claim, or the factors that were considered in determining the award under 7623(a). The IRS is evaluating comments on these and other issues addressed in the proposed regulations. The increased use of debriefings noted in response to question 9 is the principal step that can be taken to increase communication with a whistleblower.

9. In the Memorandum you issued in June of 2012, you called for a debriefing of whistleblowers to be the rule, not the exception. Since the issuance of this Memorandum, has there been any evaluation of whether this policy is being followed? Please provide any information you can share that would demonstrate that debriefings have become the rule, not the exception.

Response

The number of debriefings conducted from July 1, 2012 through April 25, 2013 has more than doubled over the number conducted from July 1, 2011 through April 25, 2012 (84 vs. 37).

10. Your June 2012 Memorandum also indicated a contract for services could be entered into with whistleblowers to obtain their insights and expertise into complex technical or factual issues. How many contracts for services have been entered into with whistleblowers? Why is this tool not being put to use as called for in your Memorandum?

Response

To date, no contracts for services have been entered into with whistleblowers. The implementing regulations require that the contract for services be used only when the IRS concludes that it needs assistance. The identification of need is a "bottom-up" process, based on developments during an audit.

Questions from Senator Patrick J. Toomey

1. Both the IRS and the Social Security Administration have taken important steps in preventing and prosecuting tax fraud in recent years. However, more work needs to be done. At a time of massive deficits, tax fraud costs the federal government billions in lost revenue and undermines the integrity of our tax system. What additional steps are being taken to increase verification of W2's, taxpayer identities, IP addresses, and social security numbers to prevent tax fraud from occurring in the first place?

Response

The IRS is placing a heightened emphasis on the prevention and detection of identity theft and refund fraud on returns submitted to the IRS. We have implemented, and continue to refine, our business processes to improve identification and prevention of tax fraud.

The Electronic Fraud Detection System (EFDS) identifies potential fraudulent returns. This system relies on data mining scores, fraud models and algorithms to determine the likelihood of fraud. As part of this process, we also look for similar attributes or characteristics such as a primary address that has been used multiple times on different returns or an IP address that is consistently used in the filing of fictitious claims.

The IRS uses a process of income verification in its risk assessment of whether a return is fraudulent. We have accelerated the use of information returns (e.g., Forms W-2) in order to identify mismatches earlier. Moving this matching process forward in time has enhanced our ability to identify fraudulent tax returns before we process them.

In addition to EFDS, the IRS built identity theft screening filters to improve our ability to spot false returns before we process them and issue refunds. For example, we designed and launched new filters that flag "risk populations" or clusters of returns if certain characteristics are detected such as multiple refunds into a single bank account or to a single address. While the development of effective filters is complex given the dynamic lives of legitimate taxpayers, these filters enable us to identify fraudulent returns even where a taxpayer's information has not been previously used for filing by an identity thief.

One of our primary strategies to assist past victims of identity theft and prevent further fraudulent filings is the creation of an Identity Protection Personal Identification Number (IP PIN). The IP PIN program began in 2011 and has since been expanded and enhanced to protect victims of identity theft by creating an additional layer of security by requiring the IP PIN when filing a tax return. The IP PIN allows the IRS to more effectively identify fraudulent returns, while at the same time, validate that the return filed is the legitimate taxpayer's return. For the 2013 filing season, we issued more than 770,000 IP PINs and have improved processing of returns filed with an IP PIN. Additionally, the replacement IP PIN process (for taxpayers who lose or misplace their original IP PIN) has been significantly streamlined to provide better service. Taxpayers are asked to validate their identities by answering a series of questions for disclosure level authentication and if validated, they receive the replacement IP PIN at the point of contact.

Beginning in 2008, we implemented the use of identity theft markers which are placed on a taxpayer's account to identify an identity theft incident. These markers are used to distinguish legitimate returns from fraudulent returns and prevent victims from facing the same problems every year. The markers provide additional protection from identity thieves by systemically evaluating taxpayers' future returns to check for inconsistencies and discrepancies that indicate potential fraudulent filing.

We are also attempting to prevent the growing misuse of decedents' social security numbers by detecting and stopping potentially fraudulent returns. We are coding the accounts of deceased taxpayers who were previously victimized and where there is no longer a future filing requirement. This coding "locks" a taxpayer's account, preventing the acceptance of potentially fraudulent returns. In addition, the President's Budget for FY2014 includes a legislative proposal that would restrict immediate access to the list of deceased individuals' SSNs known as the Death Master File (DMF) maintained by the Social Security Administration to those users who legitimately need the information for fraud prevention purposes and would delay the release of the DMF for three years to all other users.

Additionally, the IRS is reducing the use of SSNs on our systems, forms, notices, and letters to protect taxpayers from identity theft. Also, as mentioned in response to question #1, the Administration's FY2014 Budget includes a legislative proposal to grant the IRS authority to require or permit truncated social security numbers on W-2 forms that employers send to employees, to reduce the risk that the information could be stolen from a paper payee statement by identity thieves.

To address tax refund fraud associated specifically with direct deposit to prepaid and other forms of debit and bank accounts, the IRS and Treasury's Financial Management Service (FMS) have collaborated with NACHA, the Electronic Payments Association, to develop an opt-in program for interested financial institutions to enable them to return ACH direct tax refund deposits if they suspect the transfers were based on fraudulent returns. The IRS Refund Return Opt-In Program will help the IRS examine the validity of refunds already issued and stop payment on or recover invalid refunds; build better pre-refund filters; and prevent future fraudulent refunds.

WRITTEN STATEMENT OF

NINA E. OLSON

NATIONAL TAXPAYER ADVOCATE

HEARING ON

"TAX FRAUD, TAX ID THEFT AND TAX REFORM:

MOVING FORWARD WITH SOLUTIONS"

BEFORE THE

COMMITTEE ON FINANCE

UNITED STATES SENATE

APRIL 16, 2013

TABLE OF CONTENTS

I. Tax Reform and Taxpayer Rights Legislation Are Overriding Priorities for Taxpayers and Tax Administration. 4

II. Recent Budget Cuts Are Impairing the IRS's Ability to Serve Taxpayers and Collect Tax. 6

III. Despite Significant Changes to the IRS's Approach to Assisting Identity Theft Victims, the IRS Remains Inundated with Identity Theft Cases and Victim Assistance Is Taking Too Long. 11

IV. To Reduce Taxpayer Burden and Cut Down on Tax Fraud, the IRS Should Be Empowered to Process Information Reporting Documents Like Forms W-2 Before Processing Tax Returns and Issuing Refunds. 16

V. Restricting Access to the Death Master File Would Eliminate a Source of Personal Data that Identity Thieves May Utilize to Commit Tax Fraud. 20

VI. State and Local Law Enforcement Agencies Should Be Restricted from Re-disclosing Taxpayer Data Obtained from the IRS. 21

VII. Taxpayers Are More Vulnerable to Incompetent and Unscrupulous Return Preparers Because of the Recent *Loving* Decision, and if the Decision Is Not Overturned by the Court of Appeals, Congress Should Act Quickly to Authorize the IRS to Reinstate Its Rules Designed to Protect Taxpayers by Improving Standards in the Tax Return Preparation Industry. 23

VIII. Conclusion 26

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

Thank you for inviting me to testify today about the 2013 tax filing season and to present a taxpayer perspective on several priority issues in tax administration.[1] As requested, I will focus much of my statement on tax fraud and identity theft, and I will also discuss the two overriding concerns in tax administration today – the need for comprehensive tax simplification and the effects of recent cuts to the IRS budget on taxpayer service and revenue collection. In this statement, I will make the following points:

1. The tax reform options paper developed by the staff of this committee last month constitutes, in my view, an excellent starting point for improving the tax system. It has been 27 years since Congress last enacted comprehensive tax reform,[2] and it has been 15 years since Congress last passed major taxpayer rights legislation.[3] There is a significant need for legislation in both areas.[4]

2. Significant reductions in the IRS's budget since 2010 are harming taxpayers and undermining the IRS's ability to raise the revenues on which the rest of government depends.[5] For calendar year 2013 (through March 30), the IRS has been unable to answer three out of every ten calls it receives from taxpayers seeking to speak with a telephone assister, and taxpayers lucky enough to get through have had to wait more than 13

[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] Pub. L. No. 99-514, Tax Reform Act of 1986 (Oct. 22, 1986).

[3] Pub. L. No. 105-206, Internal Revenue Service Restructuring and Reform Act of 1998 (July 22, 1998).

[4] For a detailed discussion of the burdens of tax code complexity and recommendations for simplification, see National Taxpayer Advocate 2012 Annual Report to Congress 3-23 (Most Serious Problem: *The Complexity of the Tax Code*). For a detailed discussion about the need for taxpayer rights legislation, see National Taxpayer Advocate 2011 Annual Report to Congress 493-518 (Legislative Recommendation: *Enact the Recommendations of the National Taxpayer Advocate to Protect Taxpayer Rights*).

[5] In our most recent report, I designated the inadequacy of funding for the IRS as one of the most serious problems facing taxpayers. *See* National Taxpayer Advocate 2012 Annual Report to Congress 34-41 (Most Serious Problem: *The IRS Is Significantly Underfunded to Serve Taxpayers and Collect Tax*).

minutes on hold.[6] From a taxpayer perspective, this state of affairs is unacceptable. Moreover, it is self-defeating to apply across-the-board budget cuts to the IRS as a means to reduce the budget deficit, because the IRS collects substantially more than one dollar in federal revenue for each dollar it receives in appropriated funds. I recognize that this Committee does not have jurisdiction over the budget, but since you oversee the IRS and understand these issues well, I encourage you to work with your colleagues on the Appropriations Committee to ensure that the agency is adequately funded to do its job.

3. Tax-related identity theft continues to impose significant burdens on taxpayers and the IRS. While the IRS is taking the problem very seriously and has made some meaningful improvements in its processes, I remain deeply concerned that victims often have to wait in excess of six months to have their cases resolved and receive their refunds, and the IRS has yet to implement an effective program for overseeing cases with multiple issues that require coordination among functions, thereby allowing too many victims to fall between the cracks of IRS bureaucracy.[7]

4. I recommend that Congress, Treasury, and the IRS develop a long-term plan to enable the IRS to process information returns, particularly Forms W-2, before it processes tax returns and issues refunds. Front-end data verification would go a long way toward eliminating tax fraud and identity theft and could substantially reduce taxpayer burden. I originally recommended these measures in my 2009 Annual Report to Congress,[8] and the IRS has since taken some steps to move forward. One obvious requirement will be for Congress to move up the statutory deadlines by which employers and other payors of income must file information reporting documents with the government. Some significant issues, including taxpayer rights concerns, remain to be studied and overcome, but I believe the benefits of front-end data verification justify making this a near-term priority.

5. I recommend that Congress take steps to restrict immediate public access to the Death Master File (DMF). The DMF is one source of information that identity thieves use to victimize taxpayers. Several proposals have been

---

[6] IRS, Joint Operations Center, *Snapshot Reports: Enterprise Snapshot* (week ending March 30, 2013). The IRS's "Level of Service" is computed based on calls received on the Accounts Management phones lines.

[7] For a detailed discussion of tax-related identity theft, see National Taxpayer Advocate 2012 Annual Report to Congress 42-67 (Most Serious Problem: *The IRS Has Failed to Provide Effective and Timely Assistance to Victims of Identity Theft*).

[8] National Taxpayer Advocate 2009 Annual Report to Congress 338-345 (Legislative Recommendation: *Direct the Treasury Department to Develop a Plan to Reverse the "Pay Refunds First, Verify Eligibility Later" Approach to Tax Return Processing*).

made that would allow DMF data to be made available to entities that have a legitimate business need for the information while curtailing general public access for several years.[9]

6. As part of the law enforcement response to tax-related identity theft, the IRS has embarked on a program of sharing taxpayer return information with state and local authorities to facilitate prosecutions. While this information-sharing program has certain benefits, I am deeply concerned that the Internal Revenue Code (IRC) § 6103 rules that require IRS employees to keep taxpayer return information confidential do not apply to state and local authorities. With hundreds of smaller municipal governments now receiving tax return information, it is only a matter of time before one or more local officials – who unlike IRS employees do not receive regular training about the importance of protecting this information – use tax return information carelessly or inappropriately. I have raised this concern with the IRS, and its position seems to be that there is no problem because it only releases tax return information if a taxpayer executes a consent form. While it is true that the IRS is releasing return information only when taxpayers sign consent forms, my position is that most taxpayers are not experts on confidentiality waivers and may assume that state and local law enforcement authorities have the same legal obligations as IRS employees to keep their tax information confidential. It is critical that safeguards be put in place immediately to prohibit law enforcement authorities who receive tax return information for a specified purpose from using or re-disclosing that information for any other purpose without additional taxpayer consent.

7. Since 2002, I have recommended that tax return preparers be required to register with the IRS, pass a basic competency test, and take continuing education courses in order to improve industry standards and protect taxpayers from preparer errors.[10] In 2010, the IRS began to implement such a program, but a U.S. District Court recently held that the IRS lacks the legal authority to do so.[11] The Justice Department has appealed the case to the U.S. Court of Appeals for the District of Columbia, and there is a reasonable chance the D.C. Circuit will reverse the lower court decision. If it does not, however, I recommend that Congress move quickly to grant

---

[9] National Taxpayer Advocate 2011 Annual Report to Congress 519-523 (Legislative Recommendation: *Restrict Access to the Death Master File*); Department of the Treasury, General Explanations of the Administration's Fiscal Year 2014 Revenue Proposals 203 (Apr. 2013); Identity Theft and Tax Fraud Prevention Act of 2013, S. 676, 113th Cong. § 8 (2013).

[10] *See* National Taxpayer Advocate 2011 Annual Report to Congress 427-436 (Status Update: *The IRS Has Made Significant Progress in Developing and Implementing a System to Register and Test Return Preparers*); *see also* National Taxpayer Advocate 2002 Annual Report to Congress 216-230 (Legislative Recommendation: *Regulation of Federal Tax Return Preparers*).

[11] *Loving v. IRS*, 111 A.F.T.R.2d (RIA) 589 (D.D.C. Jan. 18, 2013).

the IRS the authority to reinstate the program. This committee has twice approved legislation along these lines – once under Chairman Baucus[12] and before that under former Chairman Grassley.[13] The program enjoys broad support from most preparer organizations and consumer groups, and should be relatively non-controversial.

I. Tax Reform and Taxpayer Rights Legislation Are Overriding Priorities for Taxpayers and Tax Administration.

As this Committee knows, I have repeatedly designated the complexity of the Internal Revenue Code as the #1 most serious problem facing taxpayers.[14] The existing code, by our count, has reached nearly four million words and imposes unconscionable burden on taxpayers. Our analysis of IRS data indicates that individuals and businesses spend about 6.1 billion hours a year complying with tax-filing requirements. If tax compliance were an industry, it would be one of the largest in the United States. To consume 6.1 billion hours, the "tax industry" requires the equivalent of more than three million full-time workers.

I recognize that there are substantial political differences over the appropriate level of taxation and that those differences ultimately will need to be resolved. However, I believe the prospects for comprehensive structural tax reform can be improved if the tax-writing committees begin by trying to simplify the existing tax code and achieve agreement to the extent possible. Decisions about the level of taxation and tax rates could then be deferred to the end of the process.

I have recommended that tax reform be approached in a manner similar to zero-based budgeting. For purposes of discussion, the starting assumption would be that all tax expenditures will be eliminated. A tax break would then be retained only if a majority of Members are persuaded that the benefits of that break outweigh the complexity and burden it creates. In performing this analysis, we should look at each provision in the code and ask questions like:

- Does this government incentive make sense?;
- If it does, is it better administered through the tax code or as a direct spending program?; and

[12] S. 1321 (incorporating S. 832) (109th Cong.).

[13] H.R. 1528 (incorporating S. 882) (108th Cong.).

[14] See, most recently, National Taxpayer Advocate 2012 Annual Report to Congress 3-23 (Most Serious Problem: *The Complexity of the Tax Code*).

- If yes, can it be administered without imposing unreasonable burdens on taxpayers or the IRS?

Then Congress can separately consider how much revenue it wants to raise, and it can marry up this optimally-designed tax system with its revenue decisions by setting tax rates accordingly.

Because this hearing is focused on IRS issues, I will not discuss tax reform in detail in this testimony. For those interested, our recommendations are described more fully in the National Taxpayer Advocate's 2012 Annual Report to Congress.

I do want to take a moment to commend the committee for the comprehensive tax reform options paper it released on March 21. Among tax reform proposals I have seen over the years, this options paper is unusual in that it focuses heavily on the IRS and tax administration. In my view, that makes good sense because the filing of a tax return with the IRS is where the rubber meets the road for taxpayers, and if the filing process for taxpayers can be simplified, that will go a long way toward reducing taxpayer burden.

I also want to take note that the options paper includes a mention of updating taxpayer rights legislation. Congress passed significant taxpayer rights legislation in 1988, 1996, and 1998. In fact, two members of this committee – Senator Portman and Senator Cardin – were lead sponsors of the IRS Restructuring and Reform Act of 1998 when they served in the House of Representatives. However, 15 years have now elapsed since we have had major taxpayer rights legislation. Our laws have not kept pace with our notions of procedural fairness in 21st century tax administration, particularly given our tax system's expanded and diverse taxpayer base and duties.

I have recommended grouping the many discrete taxpayer rights embedded in the Internal Revenue Code into ten broad categories, modeled on the U.S. Constitution's Bill of Rights, to help make existing rights clearer and help taxpayers better understand them.

In my view, taxpayers and tax administration would benefit from an explicit statement of what taxpayers have a right to expect from their government and what the government has a right to expect from its taxpayers. The categories I have suggested are as follows:

10 Taxpayer Rights. I have recommended that Congress organize taxpayer rights under the following ten broad principles: (1) right to be informed; (2) right to be assisted; (3) right to be heard; (4) right to pay no more than the correct amount of tax; (5) right of appeal; (6) right to certainty; (7) right to privacy; (8) right to confidentiality; (9) right to representation; and (10) right to a fair and just tax system.

5 Taxpayer Responsibilities. To help taxpayers understand what the law requires of them, I have also recommended that Congress organize taxpayer responsibilities under the following five principles: (1) obligation to be honest; (2) obligation to be cooperative; (3) obligation to provide accurate information and documents on time; (4) obligation to keep records; and (5) obligation to pay taxes on time.

In addition, we have made other legislative recommendations in recent years to strengthen taxpayer rights. Most are technical and relatively noncontroversial but will bring real benefits to taxpayers. I encourage the committee to move forward with taxpayer rights legislation this year.

II. Recent Budget Cuts Are Impairing the IRS's Ability to Serve Taxpayers and Collect Tax.

In my 2012 Annual Report to Congress, I warned that the significant and chronic underfunding of the IRS poses a major long-term risk to tax administration.[15] Over the past two years, Congress has cut the IRS's budget by nearly $1 billion, or almost eight percent. This includes more than $600 million in cuts in fiscal year (FY) 2013 because of sequestration and the rescission, which the IRS is struggling to absorb.[16]

Because of budget cuts, the IRS's full-time, permanent workforce was cut from about 86,000 to 79,000 employees from FY 2010 to FY 2012, a reduction of 8 percent.[17] By the end of FY 2012, the IRS had also cut its training budget compared with FY 2010 from about $168 million to about $63 million, a reduction of 62 percent,[18] and significant additional cuts are being made in FY 2013. The IRS has publicly estimated that the reduction in its training spending by the end of FY 2013 will be 83 percent.[19] As a result, the IRS has many fewer employees than it had just two years ago, and those employees – particularly newer ones – often are not receiving

---

[15] National Taxpayer Advocate 2012 Annual Report to Congress 34-41 (Most Serious Problem: *The IRS is Significantly Underfunded to Serve Taxpayer and Collect Tax*); *see also* National Taxpayer Advocate 2011 Annual Report to Congress 3-27 (Most Serious Problem: *The IRS Is Not Adequately Funded to Serve Taxpayers and Collect Taxes*).

[16] *See* Hearing Before Subcomm. on Financial Services and General Government of H. Comm. on Appropriations, 113th Cong. (2013) (statement of Steven T. Miller, Acting Commissioner of Internal Revenue), *at* http://appropriations.house.gov/uploadedfiles/hhrg-113-ap23-wstate-millers-20130409.pdf.

[17] IRS Integrated Financial System, Commitments, Obligations, Expenditures & Disbursements report. These figures track employees in "pay status" and exclude employees who were on Leave Without Pay or related statuses.

[18] IRS Integrated Financial System, Commitments, Obligations, Expenditures & Disbursements report.

[19] IRS Fact Sheet, FS-2013-05, *IRS Achieves $1 Billion in Cost Savings and Efficiencies* (April 2013), *at* http://www.irs.gov/uac/IRS-Achieves-$1-Billion-in-Cost-Savings-and-Efficiencies (last visited April 12, 2013).

the training they require to do their jobs well or assist taxpayers adequately, particularly with complex or atypical issues.

A. Taxpayer Services: Reduced Funding Means Taxpayer Needs Are Not Being Met.

I am concerned that the IRS is not receiving sufficient funds to meet the basic needs of taxpayers seeking to comply with the law. In each of the last two fiscal years, the IRS has received more than 115 million calls, a staggering volume that the IRS cannot come close to fully handling.[20] Last year, the IRS answered only about 68 percent of calls from taxpayers seeking to speak with a telephone assistor, and those who got through had to wait on hold for an average of nearly 17 minutes.[21] That level of service represents a sharp drop-off in performance compared with the IRS's high-water mark in FY 2004, when it answered 87 percent of its calls and the average hold time was just over 2½ minutes.[22]

The IRS's ability to timely process taxpayer correspondence has also diminished in recent years. Last year, the IRS received more than ten million letters from taxpayers responding to IRS adjustment notices.[23] Comparing the final week of FY 2012 with the final week of FY 2004, the backlog of correspondence in the tax adjustments inventory increased by 188 percent (from 357,151 to 1,028,539 pieces), and the percentage classified as "overage" jumped by 316 percent (from 11.5 percent to 47.8 percent).[24]

The impact of reduced taxpayer service is felt on the compliance side as well. Few individuals or businesses enjoy receiving a notice informing them that the IRS is reviewing their tax return or taking action to collect an outstanding tax liability. When that happens, however, it is essential that the taxpayer be able to talk to an IRS employee – whether to clarify what the notice says, present documentation to support the return position, or demonstrate that collection action would impose financial hardship and should not be taken. Among the consequences of budget cuts:

---

[20] IRS, Joint Operations Center, *Snapshot Reports: Enterprise Snapshot* (weeks ending Sept. 30, 2011 and Sept. 30, 2012); *see* Most Serious Problem, *The IRS Telephone and Correspondence Services Have Deteriorated Over the Last Decade and Must Improve to Meet Taxpayer Needs*).

[21] IRS, Joint Operations Center, *Snapshot Reports: Enterprise Snapshot* (week ending Sept. 30, 2012). The Accounts Management phones lines (previously known as the Customer Account Services phone lines) receive the significant majority of taxpayer calls. However, taxpayer calls to compliance phone lines and certain other categories of calls are excluded from this total.

[22] IRS, Joint Operations Center, *Snapshot Reports: Enterprise Snapshot* (week ending Sept. 30, 2004).

[23] *See, e.g.,* IRS, Joint Operations Center, *CAS Accounts Management Paper Inventory Reports: FY12 July-September Fiscal Year Comparison.*

[24] *Compare* IRS, Joint Operations Center, *Weekly Enterprise Adjustments Inventory Report* (week ending Sept. 29, 2012) *with* IRS, Joint Operations Center, *Weekly Enterprise Adjustments Inventory Report* (week ending Sept. 25, 2004).

- Taxpayers who submit documentation at the request of the IRS often wait extended periods for the IRS to respond;[25]

- Taxpayers are sometimes denied tax benefits because the IRS narrowly defines the types of supporting documentation it will accept and does not have the bandwidth to consider alternative forms of documentation;[26] and

- Centralization of some IRS functions means the loss of employees who understand local conditions.[27]

Another impact of shrinking IRS budgets is pressure to make greater use of automated processes. While automating certain routine tasks frees employees to focus on higher value activities, I am deeply concerned that automated "tools" are replacing employee judgment and in some cases failing to achieve the intended goal.[28] Taxpayers subject to enforcement action must wait longer to speak to an employee or have an employee read their letters, and they face additional burden when automation resolves their cases improperly.

B. Revenue Collection: Reduced Funding Means Reduced Revenue Collection and a Larger Budget Deficit.

Cutting the IRS budget also makes little sense from a revenue standpoint. In FY 2012, the IRS collected about $2.52 trillion[29] on a budget of about $11.8 billion.[30] That translates to an average return-on-investment (ROI) of about 214:1. The

---

[25] *See* National Taxpayer Advocate 2010 Annual Report to Congress 235-249 (Most Serious Problem: *The IRS Does Not Process Vital Taxpayer Responses Timely*).

[26] *See* National Taxpayer Advocate 2012 Annual Report to Congress, vol. 2, at 71-104 (*Study of Tax Court Cases in Which the IRS Conceded the Taxpayer Was Entitled to Earned Income Tax Credit (EITC)*).

[27] *See* National Taxpayer Advocate 2008 Annual Report to Congress 260-273 (Most Serious Problem: *The Impact of IRS Centralization on Tax Administration*).

[28] The Automated Substitute for Return program is an example of how an automated approach to enforcement creates downstream costs for the IRS. *See* National Taxpayer Advocate 2011 Annual Report to Congress 93-108 (Most Serious Problem: *Automated "Enforcement Assessments" Gone Wild: IRS Efforts to Address the Non-Filer Population Have Produced Questionable Business Results for the IRS, While Creating Serious Burden for Many Taxpayers*); *see also* National Taxpayer Advocate 2012 Annual Report to Congress, vol. 2, at 63-90 (*An Analysis of the IRS Examination Strategy: Suggestions to Maximize Compliance, Improve Credibility, and Respect Taxpayer Rights*), which notes that automation is leading to fewer personal contacts with taxpayers and lack of awareness among taxpayers that they are facing an enforcement action.

[29] Government Accountability Office (GAO), GAO-13-120, *Financial Audit: IRS's Fiscal Years 2012 and 2011 Financial Statements* 65 (Nov. 2012), *at* http://www.gao.gov/assets/650/649881.pdf.

[30] Department of the Treasury, *FY 2013 Budget in Brief, at* http://www.treasury.gov/about/budget-performance/budget-in-brief/Documents/11.%20IRS_508%20-%20passed.pdf.

marginal ROI of additional spending will not be nearly so large, but virtually everyone who has studied the IRS budget has concluded that the ROI of additional funding is positive. In 2011, former Commissioner Shulman estimated in a letter to Congress that proposed cuts to the IRS budget would result in reduced revenue collection of *seven times* as much as the cuts.[31]

Cutting the IRS budget therefore means fewer dollars to put toward deficit reduction, fewer dollars for military funding, fewer dollars for our intelligence services and embassy protection, fewer dollars for social programs, fewer dollars for infrastructure renewal, fewer dollars for medical research – in short, fewer dollars for all the things we believe as a nation we should provide for our citizens. It means real harm to real people.

If the Chief Executive Officer of a Fortune 500 company were told that each dollar allocated to his company's Accounts Receivable Department would generate seven dollars in return, it is difficult to see how the CEO would keep his job if he chose not to provide the department with the resources it needed to collect its receivables. Yet that is exactly what has been happening with respect to IRS funding for years, and there has been little effort to fix this obvious problem.

Because subjecting the IRS to across-the-board cuts designed to reduce the budget deficit has the opposite effect of increasing the deficit, I encourage the Finance Committee to enter into a dialogue with Members of the Appropriations and Budget committees to try to come up with a new approach to funding the IRS that gives it sufficient resources to meet taxpayer needs and collect federal revenue.

C. If a "Program Integrity Cap Adjustment" Mechanism Is Used, It Should Encompass Taxpayer Service Activities as Well as Enforcement.

In an effort to address these funding challenges, several Appropriations acts in recent years have given the IRS additional funding using a mechanism known as a "program integrity cap adjustment." Under this mechanism, new funding appropriated for IRS *enforcement* programs generally does not count against otherwise applicable spending ceilings provided:

1. The IRS's existing enforcement base is fully funded; and
2. A determination is made that the proposed additional expenditures will generate an ROI of greater than 1:1 (*i.e.*, the additional expenditures will increase federal revenue on a net basis).

[31] Letter from Douglas H. Shulman, Commissioner of Internal Revenue, to the chairmen and ranking members of the House Committee on Ways and Means (and its Subcommittee on Oversight) and the Senate Committee on Finance (Oct. 17, 2011), *at* http://democrats.waysandmeans.house.gov/sites/democrats.waysandmeans.house.gov/files/media/pdf/112/Rep_Lewis_IRS_Letter.pdf. In addition to generating direct revenue, IRS compliance actions produce indirect revenue gains. Studies show that taxpayers who might otherwise be tempted to bend the rules report their income more accurately as the likelihood of an audit increases.

The Administration's budget proposal released last week recommends a change to the Balanced Budget and Emergency Deficit Control Act of 1985 to provide program integrity cap adjustments for the next 10 years.[32] While this cap adjustment mechanism may provide an easier path to providing the IRS with more resources than a fundamental change in IRS funding rules, I am concerned that taxpayer service activities have been excluded from this enhanced funding mechanism in the past. The rationale has been that the IRS is able to measure the direct ROI of its enforcement activities – *i.e.,* it can compute to the dollar the amounts collected by its Examination, Collection, and document-matching functions – but is unable to quantify the ROI of taxpayer services. Thus, it is not currently possible to document whether or to what extent its taxpayer services generate an ROI greater than 1:1.

Creating a mechanism that allows more funding for enforcement actions while excluding taxpayer service activities like outreach and education would be a mistake for two reasons. First, common sense tells us that taxpayer services are a significant driver of tax compliance and generate a very high ROI. Publishing tax forms and instructions, conducting outreach and education to taxpayers, tax preparers, and tax software manufacturers, and otherwise administering the tax filing season are absolute prerequisites for tax compliance. In general, the ROI of these service activities is probably greater than the ROI of enforcement actions, and as we document in this report, the IRS could do a lot to improve its taxpayer services if it received additional funding for that purpose.

Second, an enforcement-only cap adjustment will inherently push the IRS to become more of a hard-core enforcement agency. It should be emphasized that in FY 2011, direct enforcement revenue amounted to only $50.2 billion[33] or two percent of total IRS tax collections of $2.52 trillion.[34] The remaining 98 percent resulted from voluntary front-end tax compliance. If cap adjustments are applied solely to bolster enforcement funding, the relative allocation of the IRS budget between enforcement and taxpayer service will shift over time in a direction that causes taxpayers to fear the IRS more and voluntarily cooperate less. In our effort to enforce the laws against noncompliant taxpayers, we must take care to avoid steps that may alienate compliant taxpayers and thereby jeopardize the existing tax base.

If program integrity cap adjustments are used, I recommend that compliance measures be defined more broadly, so that they include both an enforcement

---

[32] See Department of the Treasury, General Explanations of the Administration's Fiscal Year 2014 Revenue Proposals 187 (April 2013).

[33] IRS, Fiscal Year 2012 Enforcement and Service Results, *at* http://www.irs.gov/pub/irs-news/FY%202012%20enforcement%20and%20service%20results-%20Media.pdf.

[34] GAO, GAO-13-120, *Financial Audit: IRS's Fiscal Years 2012 and 2011 Financial Statements* 65 (Nov. 2012), *at* http://www.gao.gov/assets/650/649881.pdf.

component and a service component. Because the projected ROI of many enforcement programs is high, a more broadly constructed initiative could still produce a demonstrable ROI of greater than 1:1, even if it contained service components with ROIs that are unquantifiable. [35]

III. Despite Significant Changes to the IRS's Approach to Assisting Identity Theft Victims, the IRS Remains Inundated with Identity Theft Cases and Victim Assistance Is Taking Too Long.

As I have written in my Annual Reports to Congress since 2004, tax-related identity theft is a serious problem – for its victims, for the IRS and, when Treasury funds are improperly paid to the perpetrators, for all taxpayers.[36] In general, tax-related identity theft occurs when an individual intentionally uses the SSN of another person to file a false tax return for the purpose of obtaining an unauthorized refund.[37]

For victims, the consequences can be significant. Apart from the time and frustration involved in dealing with the IRS to prove one's own identity, taxpayers generally do not receive their refunds until the case is resolved. So far this filing season, 84 percent of all returns processed have resulted in refunds, and the average refund

---

[35] In our past annual reports, we have written about local compliance initiatives the IRS has undertaken that include integrated enforcement and outreach and education components. *See, e.g.,* National Taxpayer Advocate 2008 Annual Report to Congress 176-192 (Most Serious Problem: *Local Compliance Initiatives Have Great Potential but Face Significant Challenges*). One example: In the early 1990s, the IRS launched an initiative designed to address noncompliance by fishermen in Alaska that resulted from confusion as well as community norms and attitudes. The IRS combined stepped-up enforcement activities with an extensive outreach and education campaign in remote fishing villages and on fishing vessels that included assisting with tax return preparation and training local volunteers to assist taxpayers. By the end of the initiative, the number of nonfilers among the target population declined by 30 percent. *Id.* at 177-178.

[36] *See* National Taxpayer Advocate 2012 Annual Report to Congress 42-67 (Most Serious Problem: *The IRS Has Failed to Provide Effective and Timely Assistance to Victims of Identity Theft*); National Taxpayer Advocate 2011 Annual Report to Congress 48-73 (Most Serious Problem: *Tax-Related Identity Theft Continues to Impose Significant Burdens on Taxpayers and the IRS*); National Taxpayer Advocate 2009 Annual Report to Congress 307-317 (Status Update: *IRS's Identity Theft Procedures Require Fine-Tuning*); National Taxpayer Advocate 2008 Annual Report to Congress 79-94 (Most Serious Problem: *IRS Process Improvements to Assist Victims of Identity Theft*); National Taxpayer Advocate 2007 Annual Report to Congress 96-115 (Most Serious Problem: *Identity Theft Procedures*); National Taxpayer Advocate 2005 Annual Report to Congress 180-191 (Most Serious Problem: *Identity Theft*); National Taxpayer Advocate 2004 Annual Report to Congress 133-136 (Most Serious Problem: *Inconsistent Campus Procedures*).

[37] We refer to this type of tax-related identity theft as "refund-related" identity theft. In "employment-related" identity theft, an individual files a tax return using his or her own taxpayer identifying number (usually an Individual Taxpayer Identification Number, or "ITIN"), but uses another individual's SSN in order to obtain employment, and consequently, the wages are reported to the IRS under the SSN. Unlike in 1993, when I first represented a client in an identity theft case, the IRS now has procedures in place to minimize the tax administration impact to the victim in these employment-related identity theft situations. Accordingly, I will focus on refund-related identity theft in this testimony.

amount has been nearly $2,800.[38] For low income taxpayers who qualify for the Earned Income Tax Credit, a tax refund may amount to 25 percent or more of their annual income. There is little doubt that longer case resolution times can translate to financial inconvenience and sometimes financial hardship. That is why prompt case resolution is so important.

In FY 2013, the IRS changed its strategy for assisting identity theft victims, adopting a specialized approach under which each department (or "function") that deals with identity theft created a dedicated group of employees to work on those issues. There clearly are benefits in assigning identity theft cases to a small group of specially-trained employees so they can quickly become experts in resolving these types of cases.

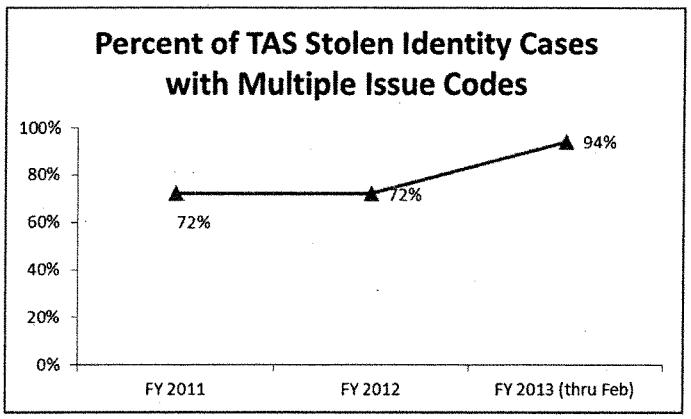
But there is another important factor that the IRS is not adequately addressing. Because identity theft cases are often very complex, they require adjustments by multiple functions.[39] The IRS has developed a "transfer matrix" outlining situations in which a case must be routed from one specialized function to another. The IRS believes that these occurrences are minimal. I disagree. Based on TAS's experience with identity theft cases over the years, I believe that transfers among functions are much more common. The vast majority of identity theft cases worked by TAS involve multiple issues,[40] as the chart below illustrates.

---

[38] IRS, Filing Season Statistics for Week Ending April 5, 2013, at http://www.irs.gov/uac/Newsroom/Filing-Season-Statistics-for-Week-Ending-April-5-2013.

[39] An IRS task force found that up to 28 different functions may touch an identity theft case. IRS, Identity Theft Assessment and Action Group (ITAAG) Future State Vision and Supporting Recommendations 7 (Oct. 11, 2011).

[40] When TAS opens a case, it assigns a primary issue code based on the most significant issue, policy or process within the IRS that needs to be resolved. When a TAS case has multiple issues to resolve, a secondary issue code will be assigned. *See* IRM 13.1.16.13.1.1 (Feb. 1, 2011).



To facilitate the transfer of such cases from one function to another, I have long advocated for the creation of a "traffic cop" to guide the case through the bureaucracy and serve as the single point of contact with the victim. Without this traffic cop, there is higher risk that cases requiring involvement of multiple functions will get "stuck" or lost in the process.

In May 2012, the Treasury Inspector General for Tax Administration (TIGTA) issued an audit report on IRS identity theft victim assistance.[41] TIGTA selected a judgmental sample of 17 identity theft cases, and its findings corroborate my position that identity theft cases are complex and vulnerable to getting lost in the IRS shuffle. TIGTA found that the IRS had opened 58 separate cases to resolve the accounts of those 17 identity theft victims – an average of nearly three and a half cases per victim.[42] The average cycle time for those cases was 414 days, which included an average of 86 days of inactivity.[43] By assigning ownership of an identity theft case to a traffic cop, the IRS can ensure that the case gets moved forward in the most efficient manner and reduce taxpayer frustration.

I have repeatedly proposed that the Identity Protection Specialized Unit or "IPSU," the centralized IRS organization established in 2008 to assist identity theft victims, could be utilized to fulfill this traffic cop role. After initial resistance, the leadership of the IRS Wage & Investment Division recently assured me that the IPSU will monitor all identity theft cases that require involvement of more than one function. For example, if a case requires the Accounts Management function to adjust the taxpayer's account, but also requires Collection to take some action, the IPSU will

[41] *See* TIGTA, Ref. No. 2012-40-050, *Most Taxpayers Whose Identities Have Been Stolen to Commit Refund Fraud Do Not Receive Quality Customer Service* (May 3, 2012).

[42] *See id.*

[43] *See id.*

ensure that the case gets routed to the appropriate place in the agreed-upon time. Furthermore, I was told that the IPSU will conduct an initial global account review upon receipt of the case to identify potential issues and then a final account review prior to case closure to determine whether all issues have been addressed. While I am pleased with this recent development, we will continue to track the IRS's implementation of these procedures. I have been recommending these changes for over five years, and it is high time that the IRS provide identity theft victims with the level of assistance they deserve.[44]

From an identity theft prevention perspective, the IRS has developed a multi-faceted approach to detecting tax returns filed by identity thieves and preventing such associated refunds from being processed. For example, the IRS utilizes a series of identity theft filters designed to detect potentially fraudulent returns, and each year it adjusts the filters as the IRS learns more about how the thieves operate. Through February 2013, the IRS stopped more than 360,000 tax returns by using these filters, an increase of more than 150 percent from the same period in 2012.[45]

The IRS also works cooperatively with banks and other financial institutions to thwart attempts by identity thieves to defraud the government. The IRS has a process by which private sector businesses, which often have developed their own algorithms to detect fraud, alert the IRS of suspicious transactions. The IRS will then investigate the taxpayers involved, and if it verifies fraudulent activity, will recoup the funds from the financial institution. Through this "external leads" program, the IRS has been able to recover over $109 million from over 30,000 accounts this year.[46]

Yet despite the revamped identity theft victim assistance procedures, more stringent filters, and improved cooperation with the private sector, the volume of identity theft returns continues to grow at an alarming rate. The IRS had more than 1.25 million identity theft cases in inventory as of the end of February 2013, a sharp increase from a year ago, when the volume was less than 235,000 cases.[47] With the average cycle time for the IRS to resolve identity theft cases exceeding six months last year,[48] I am concerned that its cycle time will skyrocket in the coming year as it struggles to keep up with its burgeoning inventory of cases.

---

[44] *See* National Taxpayer Advocate 2007 Annual Report to Congress 115 ("The IRS should develop a dedicated, centralized unit to handle all identity theft cases"); National Taxpayer Advocate 2008 Annual Report to Congress 94 ("Provide global account review and account monitoring (if necessary) for all identity theft victims").

[45] IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Mar. 28, 2013); IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Mar. 7, 2012).

[46] IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Mar. 28, 2013).

[47] IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Mar. 28, 2013); IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Mar. 7, 2012).

[48] *See* National Taxpayer Advocate 2012 Annual Report to Congress 50.

When a taxpayer whose account has been marked with an identity theft indicator fails a series of filters designed to safeguard the account (called "business rules" in IRS parlance), or if a taxpayer who was issued an Identity Protection Personal Identification Number (IP PIN) did not use a valid IP PIN when filing the return, the return will be marked "unpostable" – meaning it will not be processed. So far in this filing season, the IRS has marked 182,181 returns as unpostable, an increase of 345 percent over the same period in 2012.[49] If a taxpayer files a legitimate return that was erroneously marked unpostable, processing is delayed an average of 28 days, an increase of over 50 percent from last year.[50] Preliminary analysis suggests that an astonishing 89 percent of tax returns flagged as unpostable are eventually deemed legitimate.[51]

I am worried about the exceptionally high rate of legitimate returns becoming ensnared in the business rules. I am interested in working with the IRS to try to determine the cause of the spike in unpostable returns this year. It is not acceptable for so many legitimate taxpayers to be harmed by having their returns initially rejected and delayed nearly a month.

I have often said that TAS's case receipts are a barometer of the effectiveness of the IRS's procedures. From FY 2011 to FY 2012, TAS stolen identity cases rose by 61 percent,[52] and they have continued to trend upward this year. TAS received 26,354 identity theft cases during the first two quarters of FY 2013, a 66 percent increase over the same period in FY 2012 and a 157 percent increase from FY 2011.[53]

---

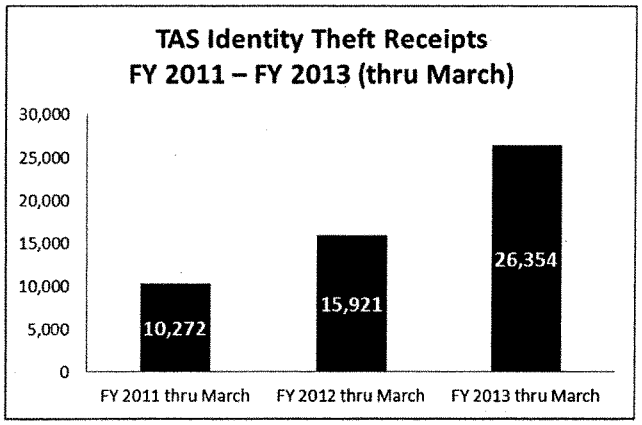
[49] The IRS is screening for more criteria that create unpostable returns in 2013 than in 2012. *See* IRS, GUF Reports 5540 and 5570.

[50] Average days to resolution for closed cases was combined with average days open or currently unresolved open cases. *See* IRS, GUF Reports 5540 and 5570.

[51] IRS, GUF Reports 5540 and 5570.

[52] Data obtained from BPMS reports on October 3, 2012, showing TAS received 34,006 identity theft cases as of September 30, 2011, and 54,748 cases as of September 30, 2012.

[53] Taxpayer Advocate Management Information System (TAMIS) (Apr. 1, 2012; Apr. 1, 2011).



The growth in TAS's identity theft casework reflects both the increase in identity theft incidents and the IRS's inability to address the victims' tax issues promptly.

IV. To Reduce Taxpayer Burden and Cut Down on Tax Fraud, the IRS Should Be Empowered to Process Information Reporting Documents Like Forms W-2 Before Processing Tax Returns and Issuing Refunds.

I have repeatedly recommended that the IRS develop a long-term plan to accelerate third-party reporting so it could match third-party data before processing tax returns and releasing associated tax refunds. Upfront matching would reduce the incidence of tax fraud, identity theft, and inadvertent errors while also providing significant taxpayer service. In particular, enabling the IRS to receive and process Forms W-2, *Wage and Tax Statement*, before releasing refunds would be an important step to deter perpetrators from committing tax fraud and identity theft. Finally, providing taxpayers and their representatives with direct electronic access to third-party data before return filing deadlines would alleviate taxpayers' burden and reduce the downstream consequences of inadvertent noncompliance.

The acceleration of third-party reporting in general would serve to increase tax compliance. Approximately 97 percent of taxpayers receive at least one information return. Traditionally, the IRS has not matched this data with the items reported on the taxpayers' tax returns until long after the filing season.[54] In 2010, the IRS closed 4.3 million cases in which it identified a discrepancy between the taxpayer's return and third-party information, leading to $7.2 billion in additional assessments.[55] The

[54] IRS, PowerPoint, Real Time Tax System Initiative, Public Meeting 2 (Dec. 8, 2011), *at* http://www.irs.gov/pub/irs-utl/rtts_deck.pdf (last visited April 8, 2013).

[55] *Id.*

real volume of mismatches is significantly larger, because this data only reflects mismatches large enough for the IRS to work, and does not include others below the IRS's established thresholds. For perspective, the IRS identified almost 23.8 million mismatches on tax year (TY) 2010 returns, but only worked about 5.3 million cases (22 percent).[56]

There is broad agreement that accelerated information reporting is necessary to increase compliance and improve taxpayer service. In my 2009, 2011, and 2012 annual reports, I wrote about the benefits of accelerated third-party information reporting to both taxpayers and tax administration.[57] In its response to the 2012 analysis, the IRS acknowledged that it had taken early steps toward the development of a real-time tax system (RTTS) with the ultimate goal of reducing taxpayer burden and increasing compliance.[58] In addition, the IRS solicited comments from a diverse group of stakeholders at two public meetings. While the participants expressed concerns about how the IRS would achieve this system, there was consensus that the goal of the initiative would serve both taxpayers and tax administration.[59]

In general, the goal of an RTTS is to enable the IRS to match information during the filing season and prior to releasing the associated refunds.[60] If the IRS identified mismatches before releasing refunds, both taxpayers and the government would avoid the subsequent consequences of assessments.[61]

An RTTS would substantially reduce taxpayer burden in several ways:

---

[56] IRS response to TAS information request (Oct. 17, 2012).

[57] National Taxpayer Advocate 2009 Annual Report to Congress 338-345; National Taxpayer Advocate 2011 Annual Report to Congress 284-295; National Taxpayer Advocate 2012 Annual Report to Congress 180-191.

[58] National Taxpayer Advocate 2012 Annual Report to Congress 190.

[59] During the meeting held on December 8, 2011, the IRS heard statements from the members of three panels: (1) tax practitioners, (2) federal and state government representatives, and (3) taxpayer and consumer advocates. During the second meeting, which was held on January 25, 2012, the IRS solicited comments from four panels consisting of (1) payroll/W-2 filers, (2) Form 1099 issuers, (3) software providers, and (4) state revenue agencies. For written and oral statements of panelists at the two RTTS public meetings, see http://www.irs.gov/Tax-Professionals/Real-Time-Tax-Initiative (last visited April 8, 2013).

[60] IRS, PowerPoint, Real Time Tax System Initiative, Public Meeting 2 (Dec. 8, 2011), *at* http://www.irs.gov/pub/irs-utl/rtts_deck.pdf (last visited April 8, 2013).

[61] When the IRS's Automated Underreporter (AUR) system identifies a mismatch between items reported on the taxpayer's return and information reports, it generates a CP 2000 notice to be mailed to the taxpayer. In TY 2010, the IRS mailed 3,823,766 of these notices to taxpayers, and the estimated response rate was 45 percent. These numbers have declined from 4,546,817 notices in TY 2009 (with an estimated response rate of 60 percent) and 4,788,360 notices in TY 2008 (with an estimated response rate of 57 percent). IRS response to TAS information request (Oct. 17, 2012) (data through Oct. 16, 2012).

- Taxpayers would be better equipped to answer questions about an underlying economic transaction if the IRS identified the mismatch within months rather than a year or more after the fact.
- Matching data before the IRS releases refunds would prevent taxpayers from facing IRS collection actions long after they have spent the refunds.
- Taxpayers would save money by avoiding the long-term accrual of penalties and interest on unintentionally omitted or under-reported items.
- Upfront matching would reduce taxpayers' vulnerability to identity-theft related refund fraud.[62]
- Giving taxpayers access to third-party data before the return filing deadline would help them prepare returns and prevent inadvertent omissions and understatements.

In addition, the government would benefit from the revenue protection aspect of upfront matching. A real-time tax system would allow the IRS to protect revenue by resolving mismatches at the outset and preventing the release of erroneous refunds. This system would deter fraud by stopping the refund associated with an upfront mismatch. Further, the IRS would devote fewer resources to compliance and collection activities on basic omission and understatement cases, and could use the savings to resolve more complex issues.[63]

Legislative action may be necessary to accelerate third-party reporting deadlines, tighten e-file mandates, and enable the IRS to receive Form W-2 data at the same time taxpayers receive the forms from their employers.[64] In this regard, I encourage Congress to consider the following issues:

---

[62] IRS, PowerPoint, Real Time Tax System Initiative, Public Meeting 2 (Dec. 8, 2011), *at* http://www.irs.gov/pub/irs-utl/rtts_deck.pdf (last visited April 8, 2013). For more information on identity-theft refund fraud, see National Taxpayer Advocate 2012 Annual Report to Congress 42-67 (Most Serious Problem: *The IRS Has Failed to Provide Effective and Timely Assistance to Victims of Identity Theft).*

[63] IRS, PowerPoint, Real Time Tax System Initiative 1, Public Meeting (Dec. 8, 2011), *at* http://www.irs.gov/file_source/pub/irs-utl/rtts_deck.pdf (last visited April 8, 2013).

[64] If certain data fields on an information return require more time to complete than others due to complexity or record-keeping issues, it may be necessary to bifurcate the information reporting deadlines. For example, if employers need more time to report pension benefit calculations, the IRS could require earlier reporting of the basic Form W-2 data such as wages and withholdings and allow employers more time to file a supplemental earnings statement with the more complicated items later. Taxpayers and the IRS would receive the information they need for return filing early in the filing season and the IRS would receive the other, more complex information soon enough for compliance purposes. This bifurcation may be relevant for the upcoming reporting requirements under the Affordable Care Act that may be critical for return filing. *See* National Taxpayer Advocate 2009 Annual Report to Congress 338-345; United States Government Accountability Office, GAO-11-747T, *Hearing*

- When the IRS identifies a mismatch between third-party data and tax return information, it is unclear what type of compliance contact the IRS would make during the filing season. In developing procedures, the extent of taxpayer burden must be a significant consideration. The extent of taxpayer burden would depend largely on the accuracy of the third-party data and on the level of staffing allocated to problem resolution when mismatches occur.

- Moving up the deadlines for employers and payors of income to submit Forms W-2 and other information returns to the government would be necessary, but earlier deadlines could also be burdensome for some filers. The IRS should continue to consult with these stakeholders to determine the best way to accomplish a real-time tax system.[65]

- Even if the reporting deadline is moved up, the IRS would still need time to process the Forms W-2 and the other information returns it receives. Therefore, consideration should be given to moving back the date for issuing tax refunds by a month or two to allow the IRS sufficient time to perform document matching and verify the accuracy of refunds claimed on filed returns.

- I would strongly caution against the expansion of math error authority to cover mismatched third-party data. I have written extensively about my concerns on this subject,[66] and these concerns were also expressed by others during the taxpayer and consumer advocate panel at the first RTTS public meeting.[67]

- As part of this initiative, I believe the IRS should provide taxpayers with electronic access to a real-time transcript of data received by the IRS to help them prepare their returns and avoid inadvertent omissions. The IRS would drive compliance rates even higher by providing a way for taxpayers to download the third-party data directly into their return preparation software and by developing an IRS-provided partially pre-populated return option. Thus, taxpayers should have the choice of one of the following ways to access third party data in preparing a tax return: (1) view and print out the third-party data to assist in return preparation, (2) download the data into commercial return

---

before the Committee on Finance, U.S. Senate on Tax Gap: Complexity and Taxpayer Compliance 14-17 (statement of Michael Brostek, Director, Tax Issues, Strategic Issues, June 28, 2011).

[65] *See* IRS Public Hearing, *Proposed Real-Time Tax System, Comments from the National Payroll Reporting Consortium* (Jan. 25, 2012).

[66] *See* National Taxpayer Advocate 2011 Annual Report to Congress 74-92; National Taxpayer Advocate 2012 Annual Report to Congress 180-191.

[67] IRS, Transcript of the Public Meeting on Real Time Tax System Initiative 92-94 (Dec. 8, 2011), *at* http://www.irs.gov/Tax-Professionals/December-8,-2011-Meeting (last visited April 8, 2013).

preparation software, or (3) pre-populate the data into an IRS-provided basic electronic tax form.[68]

V. Restricting Access to the Death Master File Would Eliminate a Source of Personal Data that Identity Thieves May Utilize to Commit Tax Fraud.

Among the proposals included in the tax reform options paper released by this committee last month was a proposal to limit access to personal identifying information, such as the Death Master File. The DMF is a list of recently deceased individuals that includes their full names, SSNs, dates of birth, dates of death, and the county, state, and ZIP code of the last address on record.[69] I have recommended that Congress pass legislation to clarify that public access to the DMF can and should be limited.[70]

The public availability of the DMF facilitates tax-related identity theft in a variety of ways. For example, a parent generally is entitled to claim a deceased minor child as a dependent on the tax return that covers the child's year of death. If an identity thief obtains information about the child from the DMF and uses it to claim the dependent on a fraudulent return before the parent (the legitimate taxpayer) files, the IRS will stop the second (legitimate taxpayer's) return and freeze the refund. The legitimate taxpayer then may face an extended delay in obtaining the refund, potentially causing an economic hardship, and will bear the emotional burden of persuading the IRS that the deceased child was really his or hers.

Legislation could relieve survivors of this burden by restricting access to the DMF to those with a legitimate business purpose, or by simply delaying release of the information for several years. Proposals introduced in recent years in both houses of Congress would limit access to the DMF.[71]

I recognize the practical difficulties of passing legislation, and am concerned that taxpayers will continue to be harmed if DMF information remains available without restriction. As I discussed in depth in prior testimony, I believe that the Social Security Administration (SSA) has the legal authority to place limits on the disclosure of DMF information administratively, given the changes in the factual and legal landscape that have taken place over the past three decades.[72] Therefore, if

---

[68] *See* National Taxpayer Advocate 2012 Annual Report to Congress 189.

[69] *See* Office of the Inspector General, SSA, Ref. No. A-06-08-18042, *Personally Identifiable Information Made Available to the General Public via the Death Master File* (June 2008).

[70] *See* National Taxpayer Advocate 2011 Annual Report to Congress 519-523 (Legislative Recommendation: *Restrict Access to the Death Master File*).

[71] *See* S. 676, Identity Theft and Tax Fraud Prevention Act, 113th Cong. (sponsored by Sen. Bill Nelson); H.R. 3475, Keeping IDs Safe Act of 2011, 112th Cong. (sponsored by Rep. Sam Johnson).

[72] For a detailed discussion regarding the application of the Freedom of Information Act to the DMF, see *Identity Theft and Income Tax Preparation Fraud*, Hearing Before Subcomm. on Crime, Terrorism,

legislation is not forthcoming, I urge the SSA to reconsider its contrary legal analysis and take steps to restrict access to the DMF.

VI. State and Local Law Enforcement Agencies Should Be Restricted from Re-disclosing Taxpayer Data Obtained from the IRS.

Taxpayers have the right to expect that any information they provide to the IRS will be kept confidential unless authorized by the taxpayer or other provision of law. The Internal Revenue Code contains significant protections for the confidentiality of returns and return information.

IRC § 6103 generally provides that returns and return information shall be confidential and then delineates a number of exceptions to this general rule. Section 6103(i)(2) authorizes the disclosure of return information in response to requests from federal law enforcement agencies for use in criminal investigations. There is no corresponding exception in IRC § 6103 that allows for the release of identity theft information to *state or local* agencies.[73] However, IRC § 6103(c) provides that a taxpayer may consent to disclosure of returns and return information to any person designated by the taxpayer.

The tax reform options paper issued by this Committee last month included a proposal for the IRS to "improve information sharing with federal, state, and local law enforcement" as a means of combatting identity theft.[74] I support this proposal for the IRS to responsibly share information pertaining to identity thieves. I note that the IRS has, in fact, implemented a program facilitating consent-based sharing of identity theft information with state and local law enforcement agencies.[75] This program, initially started as a pilot in the state of Florida but now expanded to all 50 states and the District of Columbia,[76] is an effective way for local law enforcement agencies to work with the IRS to pursue identity thieves. I believe this approach strikes an

---

and Homeland Security of H. Comm. on the Judiciary, 112th Cong. (June 28, 2012) (statement of Nina E. Olson, National Taxpayer Advocate).

[73] Note, however, that certain disclosures to state law enforcement agencies are permissible. *See* IRC § 6103(i)(3)(B)(i) (disclosure of return information, including taxpayer return information, can be made to the extent necessary to advise appropriate officers or employees of any state law enforcement agency of the imminent danger of death or physical injury to any individual; such disclosure cannot be made to local law enforcement agencies). While identity theft may cause emotional and economic injury, the typical identity theft situation does not pose an imminent danger of death or physical injury. In addition, state tax agencies routinely receive federal tax return information under IRC § 6103(d), but only for purposes of State tax enforcement.

[74] *See* Senate Finance Committee, *Simplifying the Tax System for Families and Business* (Mar. 21, 2013).

[75] *See* IRS Identity Theft Advisory Council, *Identity Theft Status Update* (Mar. 28, 2013).

[76] IR-2013-34, *IRS Expands Law Enforcement Assistance Program on Identity Theft to 50 States; Victim Assistance and Criminal Investigations Grow* (March 28, 2013), *at* http://www.irs.gov/uac/Newsroom/IRS-Expands-Law-Enforcement-Assistance-Program-on-Identity-Theft-to-50-States.

appropriate balance – protecting taxpayer return information while simultaneously giving state and local law enforcement authorities more information to help them investigate and combat identity theft.

However, I am concerned that once the information is in the hands of state and local law enforcement agencies, there is no prohibition in the tax code against redisclosure. With hundreds of smaller municipal governments now receiving tax return information, it is only a matter of time before a local official (who may not have received regular training about the importance of protecting taxpayer return information, as IRS employees do) redisclosures such information, either inadvertently or willfully. I have raised this concern with the IRS, and its position seems to be that there is no problem because it only releases tax return information if a taxpayer executes a consent form. My position is that most taxpayers are not experts on confidentiality waivers and may assume that state and local authorities have the same legal obligations as IRS employees to keep their tax information confidential. It is critical that safeguards be put in place immediately to prohibit law enforcement authorities who receive tax return information for a specified purpose from re-disclosing that information for any other purpose without additional taxpayer consent.

I have suggested that the IRS require state and local law enforcement agencies to sign an agreement that would restrict them from using IRS information for any purpose unrelated to the investigation or prosecution of the identity thief. In my initial meeting with senior IRS officials at which we discussed this disclosure initiative, I raised my concerns about protecting taxpayer information and discussed requiring a memorandum of understanding (MOU) with state and local agencies that wish to participate in the disclosure program.[77] Despite this initial conversation, I have recently been informed that the IRS believes such an approach would be administratively unfeasible, as more than a hundred state and local law enforcement agencies now participate in the program. If state and local agencies do not wish to agree to such restrictions on redisclosure, I believe the IRS has an obligation to taxpayers to refrain from sharing this information.

If the IRS continues to refuse to require that state and local law enforcement agencies enter into MOUs that explicitly prohibit the use or re-disclosure of taxpayer information for unrelated purposes, I recommend that Congress consider modifying IRC § 6103(c) to explicitly limit the use of tax return information to the purpose agreed upon by the taxpayer (*i.e.*, to allow state or local law enforcement agencies to use the information solely to enforce state or local laws) and to prohibit the redisclosure of such information.[78] Indeed, such legislation may be more effective than a contract-based approach to limiting redisclosure.

---

[77] *See* IRS, *IRS Identity Theft Future State Report* 34 (Oct. 11, 2011) (implementation step included "obtain an agreement for sharing identified data and address disclosure").

[78] *See* National Taxpayer Advocate 2011 Annual Report to Congress 505.

VII. Taxpayers Are More Vulnerable to Incompetent and Unscrupulous Return Preparers Because of the Recent *Loving* Decision, and if the Decision Is Not Overturned by the Court of Appeals, Congress Should Act Quickly to Authorize the IRS to Reinstate Its Rules Designed to Protect Taxpayers by Improving Standards in the Tax Return Preparation Industry.

Since 2002, I have advocated for the regulation of return preparers. I recommended:

- A program to register, test, and certify preparers;
- Increased penalties, and improved due diligence requirements;
- A comprehensive advertising and taxpayer education campaign focused on how to choose a competent preparer and the requirement for paid preparers to
    - sign the tax return and
    - provide a copy of the return to the taxpayer;[79]

In January 2010, the IRS published a study of federal tax return preparers which in most important respects reflected our recommendations.[80] Subsequently, the IRS issued regulations requiring that all preparers register with the IRS by obtaining a preparer tax identification number (PTIN). The IRS also required that certain preparers meet testing and continuing education requirements.[81] Implementation began with the 2011 filing season, when the IRS required paid return preparers to obtain PTINs.[82] The continuing education requirement began during the 2012 calendar year. The IRS launched the registered tax return preparer competency test in November 2011 with a deadline to take the test by December 31, 2013.[83]

---

[79] See National Taxpayer Advocate 2009 Annual Report to Congress 41-69; National Taxpayer Advocate 2008 Annual Report to Congress 503-512; National Taxpayer Advocate 2006 Annual Report to Congress 197-221; National Taxpayer Advocate 2005 Annual Report to Congress 223-237; National Taxpayer Advocate 2004 Annual Report to Congress 67-88; National Taxpayer Advocate 2003 Annual Report to Congress 270-301; National Taxpayer Advocate 2002 Annual Report to Congress 216-230; *Fraud in Income Tax Return Preparation: Hearing Before the Subcomm. on Oversight of the H. Comm. on Ways and Means*, 109th Cong. (2005) (statement of Nina E. Olson, National Taxpayer Advocate).

[80] IRS Pub. 4832, *Return Preparer Review* (Dec. 2009).

[81] Treas. Reg. § 1.6109-2(d); 31 C.F.R. § 10.2 et seq.

[82] *See* IRS News Release, IR-2010-106, *IRS Begins Notifying Tax Return Preparers on PTIN Renewals* (Oct. 25, 2010).

[83] *See* IRS News Release, IR-2011-111, *IRS Moves to Next Phase of Return Preparer Initiative; New Competency Test to Begin* (Nov. 22, 2011).

In January 2013, however, a U.S. district court judge in *Loving v. Internal Revenue Service* disagreed with the IRS's view that it has the authority to implement these requirements on its own, and it invalidated the testing and continuing education requirements.[84] The Department of Justice has appealed the district court's decision to the U.S. Court of Appeals for the District of Columbia.[85]

Regardless of the legal aspects of the *Loving* case, my main focus is the retention of minimum standards for return preparation. If the Court of Appeals reverses the district court's ruling in *Loving*, the IRS would reinstate the rules requiring certain preparers to take a competency exam and complete continuing education credits. If the district court ruling stands, I urge members of Congress to move quickly to protect taxpayers by granting the IRS the authority to reinstate the program it was in the process of implementing.

The rationale for IRS oversight is clear. Because preparers play a critical role in tax administration, it is essential that the IRS ensure preparers are competent, visible, and accountable. Without meaningful IRS oversight, anyone can hang out a shingle as a "tax return preparer" with no knowledge or experience required. The Taxpayer Advocate Service has witnessed widespread problems in the tax return preparation industry. We recently have seen many misconduct cases in which the preparer has altered return information without the client's knowledge or consent in an attempt to obtain improperly inflated refunds or divert refunds for their personal benefit.[86] In addition, problems with return accuracy and ethical standards were substantiated by a series of "shopping visits" GAO and TIGTA conducted, where auditors posed as taxpayers and visited tax return preparation businesses.[87] I believe the IRS needs to set minimum standards as a consumer protection measure.[88] Such standards also would improve professionalism and reduce preparer-facilitated noncompliance.[89]

---

[84] *Loving v. I.R.S.*, 111 A.F.T.R.2d (RIA) 589 (D.D.C. Jan. 18, 2013). The government filed a motion to suspend the injunction pending appeal. The U.S. District Court for the District of Columbia denied the motion but modified the terms of the injunction. *See Loving*, 111 A.F.T.R.2d (RIA) 702 (D.D.C. Feb. 1, 2013). On February 25, 2013, the government filed a motion for a stay pending appeal. On March 27, 2013, the U.S. District Court for the District of Columbia denied the motion for stay.

[85] *See Government Files Brief in D.C. Circuit Court in Return Preparer Oversight Case*, Tax Notes Today, 2013 TNT 62-20 (Apr. 3, 2013); *Loving v. IRS*, No. 1:12-cv-00385 (D.D.C. 2013) (USCA Case No. 13-5061).

[86] For a more detailed description of return preparer misconduct and IRS procedures to assist victims of the misconduct, see National Taxpayer Advocate 2012 Annual Report to Congress 68-94 (Most Serious Problem: *The IRS Harms Victims of Return Preparer Misconduct by Failing to Resolve Their Accounts Fully*).

[87] Government Accountability Office, GAO-06-563T, Paid Tax Return Preparers: In a Limited Study, Chain Preparers Made Serious Errors 2 (Apr. 4, 2006) (statement of Michael Brostek, Director - Strategic Issues, Before the Committee on Finance, U.S. Senate); Treasury Inspector General for Tax Administration, Ref. No. 2008-40-171, Most Tax Returns Prepared by a Limited Sample of Unenrolled Preparers Contained Significant Errors (Sept. 3, 2008).

[88] See, e.g., *Brief Amici Curiae of Former Commissioners of Internal Revenue in Support of Defendants-Appellants, Loving v. I.R.S.*, No. 13-5061 at 14 (D.C. Cir. April 5, 2013) ("[I]njunctive relief is available only once the bad acts have occurred and ... barring bad tax return preparers from striking

Preparer oversight has received widespread support from stakeholders and members of Congress, so any associated legislation should be relatively non-controversial to enact. This Committee has twice approved legislation to regulate federal tax return preparers – once under Chairman Baucus[90] and once under former Chairman Grassley.[91] The full Senate also once approved similar legislation.[92] In 2005, the House Ways and Means Subcommittee on Oversight held a hearing at which representatives of five outside organizations testified in support of regulating return preparers.[93] More recently, several bills included proposals to regulate preparers – S. 1219, the Taxpayer Protection and Assistance Act of 2007; H.R. 5716, the Taxpayer Bill of Rights Act of 2008; and S. 3215, the Taxpayer Bill of Rights of 2010.[94] Each of these proposals included provisions requiring preparers to have knowledge and skills to prepare accurate returns.

In the meantime, until either the courts or Congress reinstates the IRS's authority to require preparers to demonstrate minimum competence to prepare tax returns, taxpayers remain vulnerable to incompetent or unscrupulous preparers. Accordingly, the Taxpayer Advocate Service is working to ensure that taxpayers are vigilant when they hire an individual or firm to prepare their returns. Specifically, our communications suggest that taxpayers proactively protect themselves by taking the following steps:[95]

---

again is wholly consistent with the Treasury Department's authority to regulate commercial tax return preparers in ways reasonably designed to prevent these bad acts from happening in the first instance.").

[89] By statute, the IRS cannot require attorneys and accountants to pass the competency exam or satisfy continuing education requirements to preparer returns. *See* 5 U.S.C §§ 500(b) & (c) (granting attorneys and certified public accountants the authority to represent clients before federal agencies upon submitting a written declaration stating qualifications).

[90] S. 1321 (incorporating S. 832) (109th Cong.).

[91] H.R. 1528 (incorporating S. 882) (108th Cong.).

[92] *Id.*

[93] The organizations testifying in support of return preparer regulation were the American Bar Association, the American Institute of Certified Public Accountants, the National Association of Enrolled Agents, the National Society of Accountants, and the National Association of Tax Professionals. *See Fraud in Income Tax Return Preparation: Hearing Before the Subcomm. on Oversight of the H. Comm. on Ways & Means*, 109th Cong. (2005).

[94] S. 1219, § 4, 110th Cong. (2007); H.R. 5716, § 4, 110th Cong. (2008); S. 3215, §202. 111th Cong. (2010).

[95] *See* IRS Pub. 5074, *Protect Your Refund Poster* (distributed by the Taxpayer Advocate Service to all Taxpayer Assistance Centers, Low Income Taxpayer Clinics, and Local Taxpayer Advocate offices). See additional communications at http://www.taxpayeradvocate.irs.gov/Tax-Professionals/Tax-Preparer-Regulation (last visited April 9, 2013); http://www.taxpayeradvocate.irs.gov/Individuals/Choosing-A-Tax-Preparer (last visited April 9, 2013).

- Ask the preparer directly about his or her qualifications and experience level in preparing tax returns. The taxpayer should feel confident that the preparer possesses sufficient knowledge of relevant tax law – not merely completion of return preparation software training.

- Make sure the preparer signs the return and fills in his or her Preparer Tax Identification Number where indicated on the tax return.

- Obtain from the preparer a copy of the signed and filed return and keep the copy in the event there is a problem with the return.

In addition, consistent with my longstanding position that the IRS should mount a comprehensive taxpayer awareness campaign, I believe it is more important than ever that the IRS increase its outreach and education about choosing a preparer, with particular emphasis on the populations at most risk, such as low income taxpayers and the elderly.

VIII. Conclusion

Shrinking budgets and rising identity theft cases, among other things, are posing significant challenges for the IRS. But there are many opportunities for substantial improvement in tax administration, and in my testimony, I have tried to identify a number of positive steps Congress can take to make the most of these opportunities. Specifically, I recommend that Congress:

- Simplify the tax code to reduce burden on taxpayers and the IRS.

- Enact a Taxpayer Bill of Rights so taxpayers better understand their rights and responsibilities in dealing with the IRS.

- Work to change the rules that govern funding decisions about the IRS budget, because more IRS funding means better taxpayer service *and* more revenue (assuming the funds are well spent).

- Improve the filing season by giving the IRS access to third-party reports like Forms W-2 and 1099 before it processes tax returns and issues refunds, which has the potential to improve the taxpayer experience, improve tax compliance, and make a big dent in identity theft.

- Restrict access to the DMF so the surviving relatives of decedents are less susceptible to identity theft problems.

- Require that state and local law enforcement agencies that receive taxpayer return information to pursue identity theft crimes keep the information confidential and use it solely for its intended purpose.

- Finally, grant the IRS the authority to continue to implement its well-designed initiative to improve standards in the tax preparation industry *if* the U.S. Court of Appeals for the District of Columbia ultimately concludes that the IRS does not now have that authority.

WRITTEN TESTIMONY OF JEFFREY A. PORTER

ON BEHALF OF THE

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

UNITED STATES SENATE
COMMITTEE ON FINANCE

PUBLIC HEARING ON
TAX FRAUD, TAX ID THEFT AND TAX REFORM: MOVING FORWARD WITH SOLUTIONS

APRIL 16, 2013

Good morning Chairman Baucus, Ranking Member Hatch and Members of the Committee. My name is Jeffrey A. Porter, Chair of the American Institute of Certified Public Accountants (AICPA) Tax Executive Committee. I am a sole practitioner at Porter & Associates, CPAs, a local firm in Huntington, West Virginia, which concentrates in providing tax planning and business advisory services for local businesses and high net worth individuals. On behalf of the AICPA, I am pleased to have the opportunity to testify today at your hearing on tax fraud, tax identity theft and tax reform.

The AICPA is the world's largest member association representing the accounting profession with nearly 386,000 members in 128 countries and a 125-year heritage of serving the public interest. Our members advise clients on federal, state and international tax matters and prepare income and other tax returns for millions of Americans. Our members provide services to individuals, not-for-profit organizations, small and medium-sized businesses, as well as America's largest businesses.

Identity Theft

One of the most important topics for our members this year and a primary focus for today's hearing is identity theft. With the dramatic upturn in identity theft cases, there are a number of actions CPAs and other tax professionals can take up-front to inform clients regarding the threat posed by tax identity theft. For example, as a trusted advisor, tax return preparers can inform their clients that if they receive an e-mail or other communication that looks unusual that: (1) the Internal Revenue Service (IRS or "Service") *never* uses e-mail or social media to contact taxpayers directly; and (2) the IRS provides numerous ways for taxpayers to identify possible identity theft and telephone numbers to report it. However, some actions that tax professionals believe would reduce the threat of identity theft would require legislative or regulatory changes.

The AICPA applauds the IRS's issuance of REG-148873-09, IRS Truncated Taxpayer Identification Numbers (TTINs). The proposed regulations implement the pilot program announced in Notices 2009-93 and 2011-38, which authorize filers of certain information returns to voluntarily truncate an individual payee's nine digit identifying number on specified paper payee statements furnished for calendar years 2009-2012.

We believe the proposed regulations are a positive step towards protecting the privacy and security of personal information. Over the last few years, we urged the IRS to make the taxpayer identification number truncation initiative permanent, as opposed to remaining a pilot program.[1] We appreciate that the proposed regulations: (1) make the truncation program permanent; and (2) extend the scope of the IRS truncation program to permit filers to furnish payee statements electronically. However, we support an extension of the truncation program to permit the use of truncated social security numbers (SSN) on all types of tax forms and returns provided to a taxpayer, employee or other recipient. Unfortunately, as described in more detail below, there may be current statutory or other limits placed upon the IRS's ability to expand the truncation initiative.

[1] The AICPA most recently submitted comments on truncated taxpayer identification numbers to the Internal Revenue Service on February 20, 2013.

Under section 301.6109-4 of the proposed regulations, an IRS TTIN is defined as an "individual's SSN, IRS individual taxpayer identification number (ITIN), or IRS adoption taxpayer identification number (ATIN) that is truncated by replacing the first five digits of the nine-digit number with Xs or asterisks." However, the preamble of REG-144873-09 expressly states that the IRS's ability to extend the truncation program to a greater number of payee statements by regulation is limited by statute. Thus, the proposed regulations do not extend truncation of taxpayer identification numbers beyond certain types of information returns already permitted under the pilot program.

We understand that limitations exist currently with regards to truncation on a Form W-2, *Wage and Tax Statement*. Under Internal Revenue Code (IRC or "Code") section 6051(a)(2),[2] employers are required to provide employees a written statement (i.e., Form W-2) with certain information including the employee's SSN. We urge Congress to consider a legislative proposal to change the section 6051 reporting requirement to permit truncation of employee SSNs on all copies other than the copy filed with the U.S. Social Security Administration (SSA).

In the General Explanations of the Administration's Fiscal Year 2014 Revenue Proposals, a revision to section 6051 is proposed to require employers to include an "identifying number" for each employee, rather than an employee's SSN, on a Form W-2. We generally support this concept, but strongly believe there is a need for more extensive legislation to extend the use of truncated SSNs to all types of tax forms and returns provided to a taxpayer, employee or other recipient. For example, tax preparers are required to obtain a Form 8879, *IRS E-file Signature Authorization*, from their clients in order to e-file their tax returns. This form is not submitted to the IRS, but merely retained in the tax preparer's records. However, the tax preparer must list a client's full social security number on the form and send the document to the client for signature. Then, the client will sign the form and return it to their tax preparer often through the U.S. mail or by scanning the document and submitting it via e-mail. Either process makes the client's SSN susceptible to theft. Because the form is not submitted to the IRS, or any agency for that matter, we do not believe a SSN should be required on the form.

Clearly, the need for this expansive legislation is supported by the growing concern over identity theft in general and the growth in the number of such cases being handled by the IRS. This important change to the current law will not solve all of our country's growing problems with identity theft; however, it will likely help tax practitioners from inadvertently providing criminals access to clients' identification numbers merely by sending their clients completed IRS forms.

Finally, the AICPA supports civil penalties for tax-related identity theft, including penalties on fraudulent tax preparers.[3] In the 112th Congress, Representative Erik Paulsen introduced H.R. 5630, Fighting Tax Fraud Act of 2012, which would have amended section 6694 subsections (c), (d), (e) and (f) to provide an increased penalty in certain cases of a fraudulent understatement of a taxpayer's liability by a tax return preparer. This bill was in response to the National Taxpayer Advocate's 2011 Annual Report to Congress (pages 558-561), which noted a small number of tax return preparers defraud taxpayers and the IRS by altering the taxpayers' returns without their knowledge. In many cases, preparers claimed increased refunds – that the taxpayers

[2] All references in this letter to the Internal Revenue Code are to the Internal Revenue Code of 1986, as amended.
[3] The AICPA submitted comments to the House Committee on Ways and Means Chairman and Ranking Member on July 16, 2012.

were not entitled to receive – in order to pocket the extra money themselves. The AICPA fully supports efforts, such as H.R. 5630, to deter such outrageously unethical behavior. More recently, the Administration has proposed a similar provision which would assess a civil penalty in the amount of $5,000 on an individual who files a fraudulent tax return in tax identity theft cases.[4]

Tax Filing Season

Before addressing the other issues identified for this hearing, I would like to share our feedback on this year's tax filing season, as I know that the Committee generally seeks feedback immediately after the April 15th filing deadline. Overall, it was an extremely challenging and compressed tax season for both the IRS and tax practitioners.

We appreciate the tremendous challenges the IRS faces in administering the tax filing season each year, which includes the timely release of forms, the testing of systems, and responding to taxpayer inquiries. However, when the IRS experiences a significantly challenging filing season like this one, the challenge is not limited to the government. The adverse impact extends to taxpayers and tax return preparers who face additional burdens attributable to the disruption to normal and efficient work streams and planning. In this context, our members and their clients faced a very compressed and difficult filing season this year due to the late (January 2) enactment of tax legislation and the resulting delay in the release of 31 tax forms.

Since the IRS could not accept tax returns that included certain forms until February or early March, our members essentially lost the first half of filing season. The release of forms at such a late date also necessitated the filing of more extensions of time for filing tax returns on behalf of their clients; however, extensions do not completely solve the problem. Tax preparers still needed to perform the necessary preliminary work to calculate the amount of the tax payment due with the extension. The late enactment of the law that caused these forms delays was disruptive to accounting firms' internal procedures, causing many firms to first conduct this initial review process involving the extension now, and then a second preparation and review process later to ensure proper completion of the tax return.

The delay in the release of forms also caused significant anxiety for taxpayers. In my own practice, I had over 50 tax returns substantially completed and waiting for the IRS to release one or more forms. Many of these taxpayers were anxious to file their tax returns, calling me on a weekly and sometimes daily basis to obtain an update on their returns. The delay created an aura of confusion, particularly for my elderly clients, and sometimes required additional efforts by them. Many of my clients needed to come back to my office to pick up a completed copy of their tax return; other clients needed to make an additional trip to sign the Form 8879, *IRS E-file Signature Authorization*.

Nevertheless, we believe the IRS did an outstanding job under the difficult circumstances. The IRS maintained an open dialogue with stakeholders during the entire filing season and we applaud their responsiveness to our concerns. On February 15, 2013, the AICPA submitted a letter to Acting Commissioner Steve Miller regarding the delayed release in forms. Within days, the IRS issued Notice

[4] Department of the Treasury, General Explanations of the Administration's Fiscal Year 2014 Revenue Proposals, page 212.

2013-24 in response to our concerns, which provided the appropriate relief requested from late-payment penalties assessed under IRC section 6651(a)(2).

Unfortunately, in addition to the late release of IRS forms, the filing season was a tremendous challenge to practitioners due to the late issuance of corrected Forms 1099-B, *Proceeds from Broker and Barter Exchange Transactions*, and amended Forms 1099-DIV, *Dividends and Distributions*, by an increasing number of brokerage firms. A copy of Forms 1099-B and 1099-DIV (hereinafter referred to as "Form 1099") must be furnished to taxpayers by February 15, 2013.[5] However, brokerage firms can amend a Form 1099 at any time. In fact, one of the largest brokerage firms issued corrected Forms 1099 on April 2nd of this year. I was first notified about this brokerage firm's late corrected Form 1099 on April 4th when I began receiving calls from clients – merely eleven days prior to the initial filing due date – asking me to amend their individual income tax returns that had already been prepared and filed. Although an amended Form 1040 can be filed after April 15th, clients wanted to either make certain they did not owe any late payment penalties or obtain their refund as soon as possible. Taxpayers were also anxious to get this year's tax return "behind them" without extensions, if possible.

Over the last few years, we have noticed more and more brokerage firms issuing corrected Forms 1099, sometimes issuing multiple corrected forms on the same account. While we understand that the brokerage firms face many challenges to meet reporting requirements in a timely fashion after close of the calendar year, corrected forms create anxiety, confusion and for some taxpayers, an increase in tax preparation fees. Taxpayers are willing to file an amended return if necessary, but strongly prefer to file only once. As a result, many taxpayers (including a lot of my clients) now have a tendency to wait until they have received their annually-anticipated corrected Forms 1099 before bringing their tax records to their CPA. For example, last year I prepared an individual income tax return for one of my elderly clients on February 12th, and had to amend the return in April due to an amended Form 1099. This year, he did not want to send me his tax information in February because he was concerned about possibly receiving a corrected Form 1099. The client's prediction, or educated guess, was correct, and he received several corrected Forms 1099. He eventually brought me his tax information, and I prepared his individual income tax return this year on April 3rd – nearly two months after the date when I had prepared it in the past. Such compression in the tax filing season is becoming a reality more and more for tax practitioners each year. According to IRS statistics, returns prepared by tax professionals through March 15, 2013 had decreased by 8.1 percent from the 2012 filing season.[6]

We believe there is a solution to the growing problem of corrected Forms 1099. We suggest you consider legislation that would permit taxpayers to report *de minimis* changes in their income from a corrected Form 1099 or amended Schedule K-1 (from a partnership, trust, or S Corporation) in the year of receipt of the amended form. For example, if ordinary dividends of $200 are reported on my client's tax return for 2012, the client should not need to file an amended tax return if the client receives a corrected Form 1099 showing $210 of dividends. Such a process is inefficient for taxpayers, tax preparers and the government.

---

[5] IRC section 6045(b).

[6] IRS Filing Season Statistics for Week Ending March 15, 2013, available at http://www.irs.gov/uac/Newsroom/Filing-Season-Statistics-for-Week-Ending-March-15-2013.

The IRS could provide a simple one-page form allowing taxpayers to report the amount shown on the taxpayer's original return and the amount reported on a corrected or amended form. The differential would be included on the taxpayer's current year return (i.e., if a taxpayer receives a corrected Form 1099 in April 2013 for the 2012 or prior tax year, the taxpayer would report the difference on the taxpayer's 2013 income tax return). Because the change in income would be attributable to a corrected or amended form (as opposed to taxpayer error), good faith would automatically be presumed and late-payment penalties should not be assessed. Taxpayers would also have the option of filing an amended return.

The AICPA proposes this flexibility to streamline the tax return reporting process for both the government and taxpayers. The preparation, filing, processing and examining of amended returns is costly to everyone. This recommendation would make the entire process more efficient.

Preparer Registration

Another important item included in the topics for today's hearing is tax reform – which includes an issue of particular interest to our members – the regulation of tax return preparers. Obviously, clarity in this environment is necessary due to the pending judicial situation. The AICPA has always been a steadfast supporter of the IRS's overall goals of enhancing compliance and elevating ethical conduct. Ensuring that tax preparers are competent and ethical is critical to maintaining taxpayer confidence in our tax system. Indeed, these goals are consistent with AICPA's own Code of Conduct and enforceable tax ethical standards.

We believe the IRS should be commended for its efforts in the implementation of their return preparer program. Specifically, the IRS devoted an unprecedented amount of time to listening to stakeholder concerns and suggestions regarding the program, and made numerous changes and adjustments. We believe some of those changes confirm the Service's recognition of the inherent regulatory regime within which CPAs and other Circular 230 legacy practitioners already practice, as well as the fact that CPA firms must stand, as a matter of licensure, behind the work performed by the members and employees of the firm. We believe these changes appropriately focused the program on the "unenrolled" preparer community that was implicated in the U.S. Government Accountability Office (GAO) and U.S. Treasury Inspector General for Tax Administration (TIGTA) compliance studies cited in the IRS's preparer regulation report.

The AICPA generally supports the IRS tax return preparer program. Specifically, we support:

- Registering paid tax return preparers and the issuance of unique preparer tax identification numbers. Registration will allow the accumulation of important data on specific preparers, as well as classes of preparers in a way that will allow the IRS to tailor compliance and education programs in the most efficient manner.
- Expanding the ethical umbrella of Circular 230 over all paid income tax preparers. "Unenrolled" preparers had previously not been subjected to the ethical guidance of Circular 230 nor its sanctions for improper conduct.
- Creating a continuing education and competence construct geared towards the "unenrolled" preparer community who prepare Form 1040 series returns. Including a focus on the basics is the correct remedial approach for the "unenrolled" preparer community that was, again, implicated in the GAO and TIGTA compliance studies.

- Recognizing the potential for taxpayer confusion regarding the relative qualifications of different paid preparers through the issuance of Notice 2011-45, which constrains "registered tax return preparers" from misleading advertising and solicitation and will require these preparers to use the following statement in ads: 'The IRS does not endorse any particular individual tax return preparer. For more information on tax return preparers go to IRS.gov.'" We also believe that any public-facing IRS sources concerning preparers should contain sufficient information that taxpayers will need to make appropriate choices concerning the selection of a tax adviser. IRS mitigation of any taxpayer confusion regarding relative qualifications should be a critical and ongoing component of any program.

We will continue to provide feedback on the work the IRS undertakes with regard to its tax preparer program as we share the Service's interest in improving tax administration and protecting the taxpaying public.

Penalty Reform

Another important item for inclusion in today's tax reform discussions is the reform of penalties. The success of our tax system depends on voluntary compliance with the tax laws. "Civil tax penalties should exist for the purpose of encouraging voluntary compliance and not for other purposes, such as the raising of revenue."[7] Twenty-four years ago, Congress enacted the Improved Penalty and Compliance Tax Act of 1989 (IMPACT),[8] which overhauled the then-existing civil tax penalty regime and reiterated that the core goal of penalties is to encourage voluntary compliance. Unfortunately, in the 24 years since IMPACT, numerous penalty provisions have been enacted that are not directed toward, and do not achieve, the core goal of encouraging voluntary compliance. In part, this occurrence likely is due to the government's understandable interest in combating tax shelters. However, this loss of direction also has resulted from ad hoc efforts to craft penalties and an increase in the use of penalties, rather than altering the actual tax laws, to drive taxpayer behavior. The use of penalties to "raise revenue" contributes to this loss of direction.

Civil tax penalties should be fair, above all else. Penalty provisions should be carefully crafted by Congress and sensibly administered by the IRS to ensure that penalties deter bad conduct without deterring good conduct or punishing the innocent (i.e., unintentional errors). Targeted, proportionate penalties that clearly articulate standards of behavior and that are administered in an even-handed and reasonable manner encourage voluntary compliance with the tax laws. On the other hand, overbroad, vaguely-defined, and disproportionate penalties, particularly those administered as part of a system that automatically imposes penalties or that otherwise fails to provide basic due process safeguards, create an atmosphere of arbitrariness and unfairness that are likely to discourage voluntary compliance.

Earlier this year, the AICPA developed legislative suggestions and updated a *Report on Civil Tax Penalties: The Need for Reform* (AICPA Report) to express our concerns about the current state of civil tax penalties and to offer suggestions for improvement. Specifically, the AICPA Report addresses the following issues:

- The trend away from voluntary compliance as the primary purpose of civil tax penalties;

[7] Commissioner's Executive Task Force on Civil Penalties, Internal Revenue Service, *Report on Civil Tax Penalties*, p.1 (February 21, 1989), available at 89 TNT 45-36, Doc 89-1586.
[8] P.L. 101-239, 101st Cong., 1st Sess. (1989).

- The lack of clear standards in some penalties;
- The fact that some penalties are disproportionate both in amount and severity;
- The fact that some penalties are overbroad, deter remedial and other good conduct, and punish innocent conduct;
- The trend toward strict liability;
- An erosion of basic procedural due process;
- Inconsistencies between penalty standards and the role of tax professionals;
- The increase in the automated assessment of penalties that can lead to unwarranted assessments;
- The need for better coordination and oversight of penalty administration;
- The bias in favor of asserting penalties;
- The need to improve IRS guidance and training; and
- The need for the IRS to increase its efforts to educate taxpayers and tax professionals.

The AICPA provides its thoughts in this area with an eye toward improving overall tax policy and administration. To that end, we strongly encourage an inclusive and transparent framework for approaching this difficult task, similar to the collaborative efforts that culminated in IMPACT. We urge Congress to work with taxpayers, practitioners, professional organizations and other stakeholders in developing a systematic and thoughtful approach to civil tax penalty reform and penalty administration.[9]

Information Reporting

Another important area to discuss in addressing the administration of the tax laws is information reporting. The Code includes several requirements for payors to issue information reports to taxpayers who have received some form of taxable income. For example, section 6041, *Information at Source*, requires persons engaged in business to issue a Form 1099 to others who they have paid at least $600 of "rent, salaries, wages, premiums, annuities, compensations, remunerations, emoluments, or other fixed or determinable gains, profits, and income" during the year (unless some other reporting rule applies). Some provisions, such as section 6050W, *Returns Relating to Payments made in Settlement of Payment Card and Third Party Network Transactions*, require certain third parties to issue information reports. For example, under section 6050W, processors of debit and credit card transactions are required to issue information reports (Form 1099-K, *Payment Card and Third Party Network Transactions*) to merchants.

As noted by the GAO, "taxpayers are much more likely to report their income accurately when the income is also reported to the IRS by a third party. By matching information received from third-party payors to amounts payees report on their tax returns, the IRS can detect income underreporting, including the failure to file a tax return."[10]

In considering any potential modifications to Form 1099 or similar reporting, we think the Committee may want to review the following factors in deciding how to address the effectiveness of information reporting:

---

[9] See the AICPA tax penalties legislative proposals, submitted to Congress in April 2013, included in the submission with the April 2013 updated AICPA Report on Civil Tax Penalties.

[10] GAO, 2012 Annual Report: Opportunities to Reduce Duplication, Overlap and Fragmentation, Achieve Savings, and Enhance Revenue, GAO-12-342SP (Feb. 2012), pages 285-286; available at http://gao.gov/assets/590/588818.pdf.

- Provide exceptions for the issuance of Form 1099 to publicly-traded corporations;
- Simplify the Form 1099 issuance process for small businesses and landlords, such as considering whether it is feasible for the IRS to create a website where the data can be entered and the Form 1099 generated and mailed by the IRS to the payee; and
- Maintain the $600 threshold for filing information reports (Forms 1099). While there may be some interest in adjusting the dollar amount to account for the effects of inflation since section 6041 was enacted, given that the purpose of section 6041 is to improve compliance, the dollar amount should not be increased.

The AICPA also recommends further study and review of the efficacy of section 6050W, which pertains to returns relating to payments made in settlement of payment card and third party network transactions. It requires information reporting by payment settlement entities which process credit and debit cards for merchants. It also requires the reporting of transactions using third party networks (such as Paypal) unless they are *de minimis*.[11] Alternatives should be explored for finding businesses that might not be reporting sales, such as, those selling through third-party websites. Alternatives may also include information sharing with states and IRS examinations (correspondence and office) of individuals who sell goods or provide services via the web.

The AICPA recommends addressing sources of the tax gap through the consideration of information reporting options. As noted on the IRS Tax Gap map, the most significant way to reduce the tax gap would be to reduce its largest piece – underreporting of business income. The GAO has offered several suggestions, including ones dealing with expanded information reporting.

New information reporting requirements to help reduce this portion of the tax gap was also generated by the National Taxpayer Advocate in the 2012 annual report to Congress. This report includes the results of an independent survey to identify factors that influence voluntary compliance by small businesses. Taxpayers in the high compliance group had greater trust in the government and were likely to rely on preparers. Those taxpayers in the low compliance group tended to be suspicious of government, view the tax system as unfair, and were less likely to follow the advice of their preparer. Both compliance groups viewed the tax system as complex and cheating as wrong.[12] This additional information should be considered along with information from the IRS, GAO and others to develop administrative and legislative proposals to reduce the largest portion of the tax gap.

We believe information reporting can assist voluntary compliance by providing summary information to taxpayers for reporting on their tax returns. Accordingly, the AICPA recommends the following measures for the Committee's consideration in addressing the tax gap:

---

[11] Per section 6050W(e), a third party network transaction is *de minimis* if the potential amount to report is $20,000 or less and the number of transactions does not exceed 200.

[12] National Taxpayer Advocate's 2012 Annual Report to Congress, Vol. 2, Factors Influencing Voluntary Compliance by Small Businesses: Preliminary Survey Results; available at http://www.taxpayeradvocate.irs.gov/userfiles/file/Full-Report/Research-Studies-Factors-Influencing-Voluntary-Compliance-by-Small-Businesses-Preliminary-Survey-Results.pdf

- *Simplification*: The AICPA agrees with GAO's observation that simplification of the tax system can reduce the tax gap. The complexity of the federal tax system often leads to unintentional errors and disrespect for the system.
- *Expanded math error authority*: The AICPA conceptually agrees with the GAO's suggestion that the IRS be granted greater "math error authority" to enable it to address more mistakes prior to issuance of a refund.[13] The National Taxpayer Advocate has pointed out, though, that expanded math error authority might harm taxpayer rights in some instances.[14] The IRS should be asked for specific proposals where math error authority could be broadened while still protecting taxpayer rights.
- *Regulating paid return preparers*: The 2013 GAO report notes that in generating "approximately 60 percent of all tax returns filed, paid preparers have an enormous impact on IRS's ability to administer tax laws effectively." They also note that the program has been limited by the District Court's decision in January 2013 (*Loving v. IRS* (D.C.C. 1/18/13)).[15] Our specific recommendations are provided in this testimony under the heading "Preparer Registration."

Due Dates of Tax Returns

In addressing tax reform and the administration of the Code, we also appreciate the Committee's consideration of tax return due dates. The AICPA supports S. 420, *Tax Return Due Date Simplification and Modernization Act of 2013*, introduced by Senators Enzi and Tester on February 28, 2013. This tax return due date simplification proposal has bipartisan House support and is included in H.R. 901 as well as Title II, Subtitle B, Part 2 of the House Ways and Means Committee Chairman Camp's Small Business Tax Reform Discussion Draft.

Tax return due dates have been a concern for the AICPA for several years. Under the current system, the statutory due date for partnerships to file a tax return is the same day as for trusts, many estates, and individuals, and one month after the due date for corporations. As a result of these due dates, it is almost impossible for taxpayers and practitioners to file a timely, accurate return on the original due date if they have investments in partnerships.

Taxpayers and preparers have long struggled because Schedules K-1 often arrive months after the original due date of their or their clients' returns. Late Schedules K-1 make it difficult, if not impossible, to file a timely, accurate return. Many owners in a partnership are often forced to seek extensions; a matter further complicated by the fact that partnerships sometimes also seek extensions.

S. 420 would allow for a more logical and chronologically-correct flow of information regarding due dates of returns. Data from flow-through entities would be filed before the individuals and corporations that are invested in the flow-through entities. The bill also simplifies and better aligns other types of tax return and information return reporting due dates. These changes will increase the accuracy of tax returns and reduce the need for extended or amended corporate and individual income tax returns, resolving many of the current due date problems. The bill also helps reduce the compression of filing season for practitioners preparing

[13] *Supra*, pages 231-232.
[14] National Taxpayer Advocate's 2011 Annual Report to Congress, Vol. 2, pages 74-92.
[15] *Supra*, page 231.

individual income tax returns – a serious problem noted earlier in our testimony – while holding the amount of tax liability constant for all taxpayers.

Tax Reform

The AICPA strongly supports the leadership taken by the Committee in studying tax reform and potential solutions. The proliferation of new income tax provisions since the 1986 tax reform effort has led to complex compliance hurdles for taxpayers, administrative complexity, and enforcement challenges for the IRS. According to the National Taxpayer Advocate's 2012 Annual Report to Congress, "individuals and businesses spend about 6.1 billion hours a year complying with the filing requirements of the Internal Revenue Code."[16] It also noted "the costs of complying with the individual and corporate income tax requirements for 2010 amounted to $168 billion – or a staggering 15 percent of aggregate income tax receipts."[17] We have consistently supported tax reform simplification efforts because we are convinced such actions will significantly reduce taxpayers' compliance costs, encourage voluntary compliance through an understanding of the rules, and facilitate enforcement actions.

On behalf of the profession, the AICPA is committed to assisting this Committee and Congress in the development and passage of tax reform proposals which focus on simplifying the tax system for families and businesses, including the following proposals to improve the administrability of the tax law:

- Repeal of the alternative minimum tax (AMT). AMT is one of the tax law's most complex components. AMT adjustments and preferences require taxpayers to make a second, separate computation of their income, expenses, allowable deductions and credits.
- Harmonization and simplification of education incentives. The Code contains at least 14 complex incentives to encourage saving for and spending on education. Requirements, eligibility rules, definitions, and income phase-outs vary from incentive to incentive.
- Enactment of consistent definitions. There are several terms that have multiple and inconsistent definitions in the Code (e.g., "Modified Adjusted Gross Income") which leads to confusion. Definitions should be consistent where the same term is used.
- Simplification of the "Kiddie Tax" rules. The Code taxes a portion of the unearned income of children under the age of 18 and full-time students under the age of 24 at the parents' marginal tax rate, rather than at the child's lower rate. The complexity of these provisions creates a number of challenges and the rules should be simplified.
- Simplification and harmonization of retirement plan options. The Code provides for more than a dozen tax-favored employer-sponsored retirement planning vehicles, each subject to different rules pertaining to plan documents, eligibility, contribution limits, tax treatment of contributions and distributions, the availability of loans, portability, nondiscrimination, reporting and disclosure. These provisions should be revised so they are simpler, more readily understood, easier to comply with and administer, and more effective in enabling taxpayers to accumulate significant retirement assets.
- Repeal of unused provisions ("Deadwood"). There are numerous tax provisions which are obsolete or unimportant and rarely used. Repeal of these provisions would simplify the Code.

---

[16] National Taxpayer Advocate's 2012 Annual Report to Congress, Volume 1, MSP #1 "The Complexity of the Tax Code."
[17] *Id.*

We are available and happy to meet with you to discuss the above recommendations. We strongly support the Committee undertaking a comprehensive consideration of tax reform. In this process, we recommend you consider our Compendium of Legislative Proposals which is an aggregation of over twenty provisions in the Code that need attention and are technical in nature. We also urge this Committee to review the AICPA's Tax Policy Concept Statement #1: Guiding Principles for Good Tax Policy to assist you in identifying problems in the Code as well as to test any new proposals against the principles of good tax policy.

The IRS Budget

Finally, in the Committee's review of tax fraud, identity theft and tax reform, we urge you to address the important issue of the IRS budget. We have long advocated for funding levels for the IRS that would allow the Service to efficiently and effectively administer the tax laws and collect taxes. Giving the Service the resources necessary to properly process tax returns and enforce the tax laws is vital to maintaining our voluntary compliance tax system.

The AICPA continues to express our strong support for the adequate funding of the IRS's fiscal year 2014 budget. Unfortunately, the IRS's budget has been severely challenged in recent years. The IRS received an overall budget allocation of $11.8 billion in fiscal 2012, down from $12.1 billion for fiscal 2011. The challenge for the Service is even more dramatic as the $5.3 billion enforcement budget that the Service received for fiscal 2012, was reduced by approximately $200 million from the prior year.[18] These statistics are further highlighted by the reduction in IRS employment levels to 98,000 for fiscal 2012 from 104,000 in the prior year.

The AICPA expects that the Service would identify responsible ways to allocate any additional resources it receives; and that Congress, through its oversight responsibilities, would ensure that those resources are properly utilized. Unfortunately, the budget process has become much more complicated for federal agencies in general and especially challenging for the IRS. In this context, National Taxpayer Advocate Nina Olson stated in 2011 that the most serious challenge facing American taxpayers is the combination of the IRS's expanding workload and the agency's limited resources to handle that workload.[19] Ms. Olson points out that the Service's role has expanded from one concentrated on tax collection to one focused on distributing benefits to a variety of individuals and businesses. We agree with Ms. Olson and suggest that Congress also consider the IRS's need to administer an increasing number of aspects of health care reform when addressing the agency's budget for fiscal year 2014.

The AICPA believes that the Service should be provided with the proper resources to fund its mission, which will in turn empower the Service to fulfill its customer service and enforcement responsibilities. Any increase in enforcement funding must be balanced with positive responses to the taxpaying public as customers, a balancing act that has become even more challenging for the Service when faced with the current era of "mission creep" beyond its core tax administration functions. As we have stated in the past, all

---

[18] Department of Treasury, FY 2013 Budget in Brief, at http://www.treasury.gov/about/budget-performance/budget-in-brief/Documents/11.%20IRS_508%20-%20passed.pdf.

[19] National Taxpayer Advocate's 2011 Annual Report to Congress, Volume 1, MSP #1 "The IRS is Not Adequately Funded to Serve Taxpayers and Collect Taxes."

taxpayers must have access to resources that enable them to fulfill their tax responsibilities, and adequate IRS budgetary funding must be provided to ensure this access.

* * * * *

The AICPA appreciates this opportunity to testify and we urge this Committee to consider our suggestions as Congress decides how to address the issues of tax fraud, tax identity theft and tax reform.

American Institute of CPAs
1455 Pennsylvania Avenue, NW
Washington, DC 20004-1081

May 29, 2013

The Honorable Max Baucus
Chairman
Committee on Finance
Unites States Senate
219 Dirksen Senate Office Building
Washington, DC 20510-6200

The Honorable Robert P. Casey, Jr.
Committee Member
Committee on Finance
Unites States Senate
219 Dirksen Senate Office Building
Washington, DC 20510-6200

Re: Public Hearing on Tax Fraud, Tax ID Theft and Tax Reform: Moving Forward with Solutions

Dear Chairman Baucus and Senator Casey:

Thank you again for the opportunity to testify before the U.S. Senate Committee on Finance during the April 16, 2013 hearing on the topics of tax fraud, tax identity (ID) theft, and tax reform.

In order to complete the record of the hearing, you requested a response to one question. Accordingly, I respectfully submit the following response:

Question: Your testimony includes recommendations for tax reform, including a suggestion that we simplify our education tax incentives. You point out that requirements, eligibility rules, definitions, and income phase-outs vary from incentive to incentive. Can you elaborate on these points? What would you replace these incentives with?

The American Institute of Certified Public Accountants (AICPA) supports Congress's laws and programs that provide education tax incentives to encourage Americans to seek higher education. However, we recommend several reforms, which would allow the Committee to create simplified education tax incentives to assist taxpayers in understanding the rules and comply with them in a cost-efficient manner. Such simplification would also improve the transparency and visibility of such tax provisions and allow the monitoring of compliance with the provisions. Simplification of the education-related tax provisions would increase the benefits going to the targeted taxpayers, and lower the cost of administering the tax system.

Proposal: Harmonize and Simplify Education-related Tax Provisions

Present Law

Included in the Internal Revenue Code (IRC or "Code") are education incentives that may be divided into two general categories: (1) those that are intended to help taxpayers meet current higher education expenses and (2) those that encourage taxpayers to save for future higher education expenses.

The first category includes provisions that may be divided into three main subcategories: (1) exclusions from taxable income such as scholarships (section 117), employer-provided education assistance (section 127) and working-condition fringe benefits (section 132); (2) individual deductions, including the student loan interest deduction (section 221) and the tuition and fees deduction (section 222); and (3) individual credits, including the American Opportunity Tax Credit (previously the Hope Credit) and Lifetime Learning Credit (section 25A).

The second category, intended to fund future education, includes educational savings bonds (section 135), qualified tuition programs (section 529), and Coverdell Education Savings Accounts (section 530).

The various provisions contain numerous and differing eligibility rules for the provisions.

Description of Proposal

Tax benefits for higher education should be simplified and harmonized.[1] Specifically, we recommend the following provisions:

1. Replace tax incentives (i.e., Hope Credit, American Opportunity Tax Credit, Lifetime Learning Credit and the tuition and fees deduction) intended to help taxpayers meet current higher education expenses with one new or revised credit, and provide for an appropriate transition period. Combining features of these into one credit would simplify the tax benefits and remove duplicative provisions relating to higher education expenses.

    a. The credit should be on a "per student" rather than a "per taxpayer" basis, to assure every student is eligible regardless of family size.
    b. The credit should be available for any year of post-secondary education, including graduate-level and professional degree courses.
    c. The credit should be available only to students who are enrolled in a degree, certificate, or other program leading to a recognized educational credential at an institution of higher

[1] The AICPA submitted testimony to the Senate Finance Committee hearing on Education Tax Incentives and Tax Reform on July 25, 2012.

education and are carrying at least ½ the normal full-time work load for the course of study the student is pursuing.

d. The tax return reporting requirement should continue including the social security number (SSN) of the student associated with the expenses claimed with respect to the credit taken for the tax year. Accordingly, amounts claimed over time could be tracked by the student's SSN. These changes may result in improved compliance and enforcement.
e. The credit should be 100 percent refundable and phased out for high-income taxpayers. The phase-out limitations should be consistent with any other education-related incentive.
f. The credit should be claimed on the parent's return as long as the child is a qualifying dependent of the parent.

2. Create a uniform definition of "qualified higher education expenses" (QHEE) for all education-related tax provisions. Specifically, QHEE should include tuition, books, fees, supplies and equipment. Also, the terms "special needs services" and "special needs beneficiary" should be clearly defined.

3. If it is determined that phase-outs are necessary, coordinate the phase-out amounts for the student loan interest deduction and the educational savings bonds and Coverdell Education Savings Accounts exclusions with the new or revised tax credit intended to help taxpayers meet current higher education expenses. All education-related tax provisions should have the same Adjusted Gross Income (AGI) limitations. The concern for excessively high marginal rates resulting from coordinating phase-out provisions should be alleviated by substituting one credit for the several benefits that exist today. In addition, any remaining concerns could be addressed by widening the phase-out range, which would still permit coordination that could simplify matters for taxpayers and improve their understanding of eligibility.

Analysis

For many taxpayers, analysis and application of the intended incentives are too cumbersome compared with the benefits received. The Government Accountability Office (GAO) analyzed 2009 data for tax returns with information on education expenses and found that about 14 percent of filers (1.5 million of nearly 11 million eligible taxpayers) failed to claim a credit or deduction in which they were eligible. On average, these filers lost a tax benefit of $466 (GAO 12-560 Report to the Senate Finance Committee). Further, according to GAO research, although the number of taxpayers using the educational tax credits is growing quickly, the complexity of the tax provisions prevents hundreds of thousands of taxpayers from claiming tax benefits to which they are entitled or which would be most advantageous to them. Finally, there is evidence that the regressive nature of the provisions prevents low-income taxpayers from getting the tax benefit that Congress envisioned.

The complexity and interaction among the various provisions is a recurring theme. At the Spring 2008 House Ways and Means hearing on higher education tax incentives, Karen Gilbreath

Sowell, Treasury's deputy assistant secretary for tax policy, commented that "with more than ten million families claiming tax benefits to help finance higher education each year, Congress must ensure that these benefits work as intended" and that "the complexity of the education tax incentives increases record-keeping and reporting burden on taxpayers and makes it difficult for the IRS to monitor compliance."

For example, eligibility for one of the two education credits depends on numerous factors, including the academic year in which the child is in school, the timing of tuition payments, the nature and timing of other eligible expenditures, and the adjusted gross income level of the parents (or possibly the student). In a given year, a parent also may be entitled to different credits for different children, while in subsequent years credits may be available for one child but not another. Further complicating the statutory scheme, the Code precludes use of the Lifetime or Hope (American Opportunity Tax) Credit if the child also receives tax benefits from education savings accounts. Although the child can elect out of such benefits, this decision also entails additional analysis.

An additional complicating factor is the phase-out of eligibility based on various AGI levels in six of the provisions. This requires taxpayers to make numerous calculations to determine eligibility for the various incentives. Since there are many individual tests that must be satisfied for each benefit, taxpayers may inadvertently lose the benefits of a particular incentive because they either do not understand the provision or because they pay tuition or other qualifying expenses during the wrong tax year.

In addition to the complexity described above, there is evidence that erroneous application of education credits is making a significant contribution to the "Tax Gap." A report issued by the Treasury Inspector General for Tax Administration (TIGTA) in 2011 states that education credits of approximately $3.2 billion ($1.6 billion in refundable credits and $1.6 billion in nonrefundable credits) appear to be erroneous.[2] Over four years, erroneous education credits could potentially reach $12.8 billion.[3]

In terms of tax policy, the numerous tax incentives to assist with college expenses are not the only way the federal government provides assistance to college students and their families. Through the Department of Education, the federal government assists low-income individuals through various scholarship and grant programs. We encourage Congress to consider all of these programs together to determine if the desired goals are being met in an effective and efficient manner. The current tax provisions do not always meet the goal of helping low to middle-income families with college expenses. Consideration should be given to where assistance can best be provided through the tax law (such as incentives to save for future college expenses) versus grant and scholarship programs while the student is in college (where assistance is needed at the start of the school year rather than when the tax return is filed). Consideration should also be given to

[2] Treasury Inspector General for Tax Administration Report 2011-41-083, Billions of Dollars in Education Credits Appear to Be Erroneous (September 16, 2011).
[3] *Id.*

identifying the targeted income group to whom the federal government should be providing financial assistance for higher education expenses. When assessing whether this goal is met, aid distributed through scholarships, grants or tax provisions should be considered.

Conclusion/Recommendation

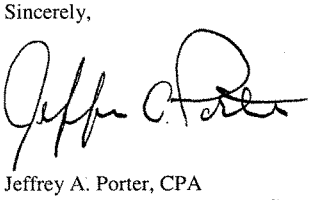
Education-related tax provisions should be simplified by the Committee, as suggested above, such that taxpayers can better understand the rules and can both claim and comply with them in a cost-efficient manner. Such simplification would also improve the transparency and visibility of such tax provisions and allow the monitoring of compliance with the provisions. Simplification of the education-related tax provisions would increase the benefits going to the targeted taxpayers, and lower the cost of administering the tax system.

* * * * *

The AICPA is the world's largest membership association representing the accounting profession, with nearly 386,000 members in 128 countries and a 125-year heritage of serving the public interest. Our members advise clients on federal, state and international tax matters and prepare income and other tax returns for millions of Americans. Our members provide services to individuals, not-for-profit organizations, small and medium-sized businesses, as well as America's largest businesses.

Thank you for considering our views on this very important topic. If you have any questions or would like to discuss this issue or our recommendations, please contact me at (304) 522-2553 or jporter@portercpa.com; or Melissa Labant, AICPA Director of Taxation, at (202) 434-9234 or mlabant@aicpa.org.

Sincerely,



Jeffrey A. Porter, CPA
Chair, AICPA Tax Executive Committee

cc: Christopher Arneson

SUBMITTED BY SENATOR WYDEN

Office of Chief Counsel
Internal Revenue Service
memorandum

Number: **201141017**
Release Date: 10/14/2011

CC:PA:07
POSTS-110431-11

UILC: 7602.03-00

date: July 08, 2011

to: Associate Area Counsel (Newark, Group 1)
(Small Business/Self-Employed)

from: William V. Spatz,
Senior Counsel, Branch 6
(Procedure & Administration)

---

subject: Summons Inquiry Regarding the Stored Communications Act
(18 U.S.C. §§ 2701-2711)

This Chief Counsel Advice responds to your request for assistance. This advice may not be used or cited as precedent.

ISSUES

1. Should the Service's administrative summons seeking from an Internet service provider (ISP) the contents of a customer's e-mails that are less than 180 days old,-- i.e., the summons requests all e-mails from a specified date through the date of the ISP's compliance with the summons – be withdrawn as inconsistent with the Stored Communications Act (18 U.S.C. §§ 2701-2711)?

2. Would it be sensible under the circumstances – in which the ISP is headquartered in the Ninth Circuit and the revenue officer is interested primarily in obtaining very recent leads to the taxpayer's potential assets from the contents of the e-mails at issue – for the Service to reissue a modified administrative summons on the ISP for the contents of the customer's e-mails that are more than 180 days old, i.e., from a specified date until another specified date that is more than 180 days before the issue date of the new summons?

3. May the revenue officer issue a modified administrative summons to the ISP for the non-content information for electronic communications services specified in 18 U.S.C.

§ 2703(c)(2) for the customer (e.g., name, address, length and type of service, and means of payment), as referred to in IRM Exhibit 5.20.4-10 (rev. 7-20-2010)?

CONCLUSIONS

1. Yes, the summons the Service issued to the ISP should be withdrawn for violating the SCA. In particular, the summons requests from a provider of electronic communication services (the ISP) the contents of electronic communications (including all e-mails) for an ISP customer that have been in electronic storage by the ISP for the 180 days preceding the Service's issuance of the administrative summons and prospectively, after the date of issuance until the date the ISP complies with the summons, in violation of 18 U.S.C. § 2703(a). This section of the SCA provides, in pertinent part, that a governmental entity may require an ISP or other provider of electronic communications services to disclose the contents of an electronic communication the ISP has maintained in electronic storage for 180 days or less, only pursuant to a warrant issued under the procedures described in the Federal Rules of Criminal Procedure by a court of competent jurisdiction. The procedures described in Federal Rule of Criminal Procedure 41 for a warrant to seek electronically stored information were not followed by the revenue officer in this case; further, the revenue officer would not be eligible to seek a warrant for the civil (as opposed to criminal) tax law provisions he is engaged in seeking to enforce in this case.

2. No, as a practical matter it would not be sensible for the revenue officer in this case to reissue a modified administrative summons to the ISP, seeking only the contents of the ISP customer's e-mails from a date certain until another specified date that is more than 180 days before the issue date of the new summons. The SCA, 18 U.S.C. § 2703(a)-(b), does permit a governmental entity to require an ISP to produce the contents of an ISP customer's electronic communications that have been in electronic storage for more than 180 days in response to an administrative subpoena (including an IRS summons). In such cases, the governmental entity must either provide prior notice of the administrative subpoena to the customer, or the governmental entity may provide the customer with "delayed notice" of the subpoena if the conditions and procedures described in 18 U.S.C. § 2705 for such delayed notice to the customer are followed, including a required written certification by a supervisory official. In a recent case, the Sixth Circuit opined that the SCA provisions which allow a governmental entity to require an ISP to produce the contents of a customer's e-mails which are more than 180 days old without a properly authorized warrant, upon a showing of probable cause, violated the Fourth Amendment (as an unreasonable search and seizure) and were unconstitutional. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010), reh'g and reh'g en banc denied, 2011 U.S. App. LEXIS 5007 (6th Cir. March 7, 2011).[1] The ISP in

[1] The Sixth Circuit went on to hold that the Government relied in "good faith" in Warshak upon the provisions at issue of the SCA – allowing the Government to obtain the contents of the e-mails at issue via a subpoena or via a court order requiring a reasonable showing of relevance and materiality to an ongoing criminal investigation (rather than "probable cause") – so the court declined to apply the "exclusionary rule" to the evidence the Government obtained via the subpoena and court order under SCA procedures. Warshak, at 288-292. Consequently, the petitions for rehearing en banc that were filed

the present case is headquartered within the Ninth Circuit, rather than the Sixth Circuit, but the ISP has advised Counsel that it does not intend to comply voluntarily with the summons. The Ninth Circuit has not yet addressed the constitutionality of the provision of the SCA that the Sixth Circuit opined was unconstitutional, but the Ninth Circuit has previously opined that the contents of certain electronic messages were protected by the Fourth Amendment, and it has discussed possible constitutional distinctions between the contents of electronic communications and the non-content information associated with a customer's use of electronic communications. In short, we do not believe there is any reasonable possibility that the Service will be able to obtain the contents of this customer's e-mails that are more than 180 days old through a modified summons upon this ISP without protracted litigation, if at all. Moreover, the revenue officer has indicated that he is primarily interested in this case in the opportunity to look for the most recent potential collection leads in the customer's e-mails. The most recent e-mails the SCA permits the Service to seek via an administrative summons would surely contain only "stale" leads by the time any protracted litigation with the ISP (and any intervenors and likely amici)[2] could practically be concluded.

3. Yes, the current controversy concerning the constitutionality under the Fourth Amendment of the SCA permitting governmental entities to obtain the "content" of more than 180-day old customer e-mails and other electronic communications from an ISP by means short of a court-approved warrant, upon a showing of "probable cause," should not affect the Service's ability to continue to use an administrative summons to obtain from an ISP the non-content records concerning a customer's electronic communication services, which are described in 18 U.S.C. § 2703(c)(2). A model summons attachment that requests this non-content information from an ISP was contained in the July 2010 version of IRM Exhibit 5.20.4.-10, which is currently being republished in IRM chapter 25.5.2. The Ninth Circuit and other courts have recognized that a warrant is not required by the Constitution for a government entity to require an electronic communications provider to produce a customer's non-content information regarding an electronic communication. See United States v. Forrester, 512 F.3d 500, 509-513 (9th Cir.), cert. denied sub. nom., 129 S.Ct. 249 (2008) (the Government's use of a court-approved computer surveillance analogue to a pen register for telephone calls, disclosing the "to" and "from" addresses for a customer's e-mail messages, was not a "search" for Fourth Amendment purposes); United States v. Bynum, 604 F.3d 161, 164 (4th Cir.), cert. denied, 130 S.Ct. 3442 (2010) (a customer's subscriber information provided to an ISP is not protected by a Fourth Amendment privacy expectation); In re § 2703(d) Order, 2011 U.S. Dist. LEXIS 25322 (E.D. Va. March 11, 2011) (the Wikileaks Twitter Order case). Pursuant to 18 U.S.C. § 2703(c)(2)(F), the Service may continue to use an administrative summons upon an ISP (with no "notice" to the affected customer) to request, inter alia, the "means and source of payment" for the ISP's

---

with the Sixth Circuit in January 2011 were filed only by defendants Warshak and his mother; the United States did not file a petition for rehearing of the Sixth Circuit's 2010 decision in Warshak.

[2] The Electronic Frontier Foundation, a privacy advocacy group, participated in an amicus role at some stages of the Warshak case, and has done so in other cases involving these SCA issues.

electronic communication services to the customer, "including any credit card or bank account number." Through follow-up requests based on this ISP customer payment information, if sought in a new summons, the revenue officer may indirectly obtain some of the potential collection asset leads he is interested in pursuing further in this case.

BACKGROUND

The Service is seeking to collect more than a quarter million dollars assessed against an apparent shell entity taxpayer which received large tax refunds, arising from improperly claimed tax credits. The revenue officer is seeking to identify sources from which collection may be made, including from the assets of a suspected alter ego of the taxpayer. To learn more about the suspected alter ego's finances, specifically to whom and where the suspected alter ego may have transferred funds, the revenue officer served a summons upon an ISP headquartered within the Ninth Circuit. The summons requests the contents of the suspected alter ego's electronic messages and other communications for a period exceeding two years, through the date of the ISP's compliance with the summons. The revenue officer indicates is particularly interested in receiving the most recent e-mails, those the suspected alter ego sent or received within the last 180 days before the ISP complies with the summons. In response to the summons, the ISP first sent the revenue officer a letter, informing him of some of the relevant SCA limitations contained in 18 U.S.C. §§ 2703(a)-(b) and 2705. In a subsequent conversation, a representative of the ISP informed Counsel that the ISP would not voluntarily comply with the summons, in large part due to the recent Warshak decision by the Sixth Circuit. You requested our advice on how to proceed with respect to the summons.

ADDITIONAL DISCUSSION

Steven Warshak, an owner/operator of small businesses, was convicted in 2008 for fraud and money laundering in connection with the false marketing of Enzyte. His criminal conduct involved a series of advertisements on television and the Internet. It also included his practice of enrolling persons who responded to the advertisements in auto-ship programs for Enzyte without their consent, and his practice of misrepresenting his businesses' chargeback records for unsatisfied customers to various merchant banks that had agreed to process the credit card payments received by the Warshak businesses. In 2004, the Government first formally requested that one of Warshak's ISPs prospectively preserve the contents of any e-mails to and from Warshak's e-mail account to prevent them from being automatically deleted (via Post Office Protocol) from the ISP's server after Warshak downloaded the messages. Next, in 2005 the Government issued a subpoena to the ISP, pursuant to 18 U.S.C. § 2703(b)(1)(B)(i), requiring the ISP to turn over the content of some of the e-mails that it had begun preserving the previous year. Several months later in 2005, the Government obtained a further ex parte court order, pursuant to 18 U.S.C. § 2703(b)(1)(B)(ii), requiring the ISP to surrender the contents of additional e-mails preserved from Warshak's account. In all, the Government compelled the ISP to reveal the contents of approximately 27,000

e-mails. Warshak did not receive notice of either the subpoena or the order until more than a year later. Warshak, at 283.

The Sixth Circuit began with the proposition that a Fourth Amendment "search" occurs when the Government infringes upon "an expectation of privacy that society is prepared to consider reasonable." The court said this standard breaks down further into two discrete inquiries, first whether the target of the investigation has manifested a subjective expectation of privacy in the object of the challenged search, and second whether society is willing to recognize that expectation as reasonable. The Sixth Circuit found that Warshak plainly manifested a subjective expectation that his e-mails would be shielded from outside scrutiny. The court found that answering whether society was willing to recognize an expectation of privacy in the contents of e-mails as reasonable was of great importance because of "the prominent role that email has assumed in modern communication" and because "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish." The Sixth Circuit looked first for guidance to the case of Katz v. United States, 389 U.S. 347 (1967), where Government agents had affixed an electronic listening device to the exterior of a public phone booth and had used the device to intercept and record several phone conversations. In Katz, the Supreme Court found that this electronic interception of the contents of a conversation constituted a "search" under the Fourth Amendment, notwithstanding the fact that the telephone company (a third party) had the capacity to monitor and record the calls for its own business reasons. The Sixth Circuit further observed that the contents of letters receive similar Fourth Amendment protection, despite the fact that sealed letters are handed over to perhaps dozens of mail carriers, any one of whom could tear open the envelopes that separate the private words from the world outside. Warshak, at 284-5.

In further support of the proposition that the contents of e-mails deserve the same societal protection from a warrantless search as the contents of traditional paper mail or a telephone conversation, the Sixth Circuit cited to portions of the Ninth Circuit's 2008 Forrester decision, which had found the non-content portions of e-mail messages (e.g., the senders and receivers) were unprotected by the Fourth Amendment, and different in character from the "contents" of the e-mails (which had not been obtained without a warrant in that case). Warshak, at 286; Forrester, at 509-10 (importantly, the Supreme Court in the pen register case of Smith v. Maryland, 442 U.S. 735 (1979), distinguished pen registers from more intrusive surveillance techniques on the ground that pen registers do not acquire the "contents" of communications, but rather only the addressing information associated with phone calls). The Sixth Circuit also relied upon findings from a Ninth Circuit case that was reversed by the Supreme Court. Significantly, the Supreme Court did not adopt those findings; instead, it chose to assume them arguendo or comment on without deciding their merits. Warshak, at 286; City of Ontario v. Quon, 130 S.Ct. 2619, 2629-30 (2010), rev'g, Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008) (explicitly assuming only arguendo that Quon had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the city, and observing that the "judiciary risks error by elaborating

too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear").

In Warshak, at 288-9, the Sixth Circuit ultimately held and announced the intended application of its decision as follows:

> The government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause. Therefore, because they did not obtain a warrant, the government agents violated the Fourth Amendment when they obtained the contents of Warshak's emails. Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional. ... However, we disagree that the SCA is so conspicuously unconstitutional as to preclude good-faith reliance. .... it was not plain or obvious that the SCA was unconstitutional, and it was therefore reasonable for the government to rely upon the SCA in seeking to obtain the contents of Warshak's emails. ... Of course, after today's decision, the good-faith calculus has changed, and a reasonable officer may no longer assume that the Constitution permits warrantless searches of private e-mails.

Since Warshak was decided, commentators and Government officials have observed that "the decision is only binding within the four states comprising the Sixth Circuit." Commentator Casey Perry opined that "it remains unclear how the rest of the nation will treat the Warshak decision," and "the good faith exception would continue to exist in each circuit until a similar case is heard and decided."[3] And in his April 6, 2011 testimony before the Senate Judiciary Committee, Cameron F. Kerry, General Counsel, U.S. Department of Commerce, stated:

> Warshak is the law only in the Sixth Circuit, and the U.S. government is determining whether to seek Supreme Court review [and] [u]ntil such time as the Court squarely addresses the issue, the law as to what protection the Fourth Amendment affords to the messages and other customer content transmitted and stored electronically will be unsettled. [4]

At the same hearing before the Senate Judiciary Committee, Associate Deputy Attorney General James A. Baker cautioned legislators to consider carefully whether the existing SCA or the Sixth Circuit's Warshak opinion strikes the correct balance about the privacy interests that society is willing to recognize as reasonable, explaining:

---

[3] U.S. v. Warshak: Will Fourth Amendment Protection be Delivered to Your Inbox?, 12 N.C. J.L. & Tech. 345, 365-6 (2011).

[4] The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Before the Sen. Judiciary Comm., Apr. 6, 2011, available at http://judiciary.senate.gov/hearings/hearing.cfm?id=e655f9e2809e5476862f735da16a199e, page 10 (Testimony of Cameron F. Kerry, General Counsel, U.S. Dept. of Commerce).

First, current law allows for the acquisition of certain stored communications using a subpoena where the account holder receives prior notice. This procedure is similar to that for paper records. If a person stores documents in her home, the government may use a subpoena to compel production of those documents. Congress should consider carefully whether it is appropriate to afford a higher evidentiary standard for compelled production of electronically-stored records than paper records.

Second, it is important to note that not all federal agencies have authority to obtain search warrants. For example, the Securities and Exchange Commission (SEC) and Federal Trade Commission (FTC) conduct investigations in which they need access to information stored as the content of email. Although those entities have authority to issue subpoenas, they lack the ability to obtain search warrants. Raising the standard for obtaining stored email or other stored communications to a search warrant could substantially impair their investigations.

Third, Congress should recognize the collateral consequences to criminal law enforcement and the national security of the United States if ECPA were to provide only one means – a probable cause warrant – for compelling disclosure of all stored content. For example, in order to obtain a search warrant for a particular email account, law enforcement has to establish probable cause to believe that evidence will be found in that particular account. In some cases, this link can be hard to establish. In one recent case, for example, law enforcement officers knew that a child exploitation subject had used one account to send and receive child pornography, and officers discovered that he had another email account, but they lacked evidence about his use of the second account.

Thus, Congress should consider carefully the adverse impact on criminal as well as national security investigations if a probable cause warrant were the only means to obtain such stored communications.

Please call me if you have any further questions.

COMMUNICATIONS

U.S. Senate

Committee on Finance

Tax Fraud and Tax ID Theft: Moving Forward with Solutions

April 16, 2013

Statement for the Record

John Runyan

Executive Director

Consumers for Paper Options

8 E St. SE

Washington, DC 20003

Phone: 202-543-0032

www.paperoptions.org

Mr. Chairman and members of the Committee, Consumers for Paper Options is an organization originally founded by businesses in the paper-based communications industry which has grown to include and work with concerned Americans, consumer organizations, seniors' groups, and all citizens who want government at all levels to make wise decisions regarding citizen access to information and services.

According to the latest US Census, some 30 percent of American households do not have internet service at home and some 45 percent of seniors don't own a computer. When the federal government adopts policies that limit access to paper-based versions of important information and services, it does so in complete disregard to the interests of millions of Americans who have not yet adapted to the digital age.

The shift to electronic tax filing has led to rampant identify theft perpetrated primarily on senior citizens, and it is undoubtedly putting millions more at risk with each passing year. Thieves are miles ahead of the security efforts of the IRS and other government agencies; they are systematically taking advantage of the shift to electronic tax filing and direct-deposited refunds to file fraudulent tax returns at the expense of both victimized seniors and the American people.

Until the IRS can develop sound solutions to prevent this epidemic of identity theft, electronic methods should not be the agency's primary means of tax collection and refund distribution, nor should citizens be forced into electronic filing against their wishes.

Identity Theft has Increased with the IRS' Dependence on Electronic Tax-Filing.

The IRS admits that identity theft is the number one tax scam for 2013, but the rise of tax-related identity theft is not new. It has been increasing in relation to the IRS' growing dependence on electronic tax-filing and the direct-depositing of refunds, which includes the use of pre-paid debit cards.

Last year, the Treasury Inspector General for Tax Administration reported that the IRS failed to identify 1.5 million fraudulent returns related to tax year 2010 (which were processed during the 2011 tax season) – sending out $5.2 billion in refunds to thieves. In giving this "conservative estimate," the Inspector General then noted that the report did not include instances where the IRS itself had determined that the return was fraudulent after sending the refund – it only chronicled undetected tax fraud. And since then, the problem has only worsened. More recently, the IRS reported that identify theft nearly tripled between 2010 and 2011, and as of December 2012, the IRS had identified nearly 1.8 million incidents of tax-related identity theft during calendar year 2012 alone.

With no end in sight, the Inspector General said last year that this identity theft could cost taxpayers $21 billion over the next five years – swamping any supposed gains from the IRS' paperless initiatives. Even more troubling, the IRS admits that the problem of identity theft is "significantly greater than the amount the IRS detects and prevents," so the actual impact is likely to be much worse.

Electronic tax-filing and the direct deposit of tax refunds have undoubtedly contributed to the epidemic of tax fraud being perpetrated in our country. Of the aforementioned 1.5 million undetected fraudulent returns processed during the 2011 tax season, 1.4 million, or 91 percent, were e-filed. Further, the IRS direct deposit program has made it far easier for thieves to steal funds related to these fraudulent returns. Of those 1.5 million undetected fraudulent returns processed during the 2011 filing season, 1.2 million (or 82 percent) utilized direct deposit (which includes the use of pre-paid debit cards) to obtain fraudulent refunds.

There is no better proof that electronic tax-filing and refund collection has played a central role in our nation's skyrocketing tax fraud. Debit cards are not a secure means of refund collection. They are untraceable, and can be collected and used without proper identification. As for funds received electronically via direct deposit, the IRS does not even mandate basic safeguards requiring the name on the bank account to match the name on the tax return.

While cashing a paper check involves protections to ensure that the funds are being received by the correct person, electronic tax-filing has empowered thieves across the country. There is no accountability at the IRS, and certainly no credible effort to prevent electronic tax-filing from resulting in the epidemic of fraud we are experiencing today.

Seniors Are the Most Likely Victims of Tax Fraud.

Seniors are disproportionately affected by tax fraud, and a prime reason is the prevalence of electronic tax-filing and refund-collection that is exposing elderly Americans – many of whom have little or no knowledge of technology or the way electronic filing works – to cybercrime.

While cybersecurity is a top concern for many American citizens, both young and old, it is a fact that senior citizens are often prime targets for cybercrime. For instance, Florida – a state with the highest percentage of elderly citizens – has the highest rate of identity theft in the nation. Nine of the 10 U.S. cities hit hardest by tax fraud are in Florida. The Miami area is the nation's number one location for this crime, with 35,914 cases of tax-related identity theft reported in 2012 and the highest per capita rate of complaints: 645 per 100,000 residents.

Seniors are particularly susceptible to fraud because many are uncomfortable in the digital world or simply unprepared for its consequences. Forty-five percent of seniors do not own a computer – indicating that they might not grasp the ease in which someone's personal information can be used for fraud. For this reason, thieves have been systematically targeting seniors across the country. Many telephone elderly Americans and tell them they are the recipients of cash prize and that they need to divulge their Social Security numbers or banking information in order to receive the winnings. And because electronic tax-filing does not involve the reliable security features of traditional filing, these thieves are able to easily file fraudulent returns using stolen information.

Just look at the Social Security Administration, which has been ignoring the preferences of millions of seniors by continuing its efforts to switch them to electronic-only federal benefits. Since this effort began, the Inspector General for the Social Security Administration has reported

a stark increase in fraud perpetrated primarily on elderly beneficiaries. In most cases, criminals obtained sensitive personal information and were able to redirect the victims' direct-deposited benefits to a fraudulent account. According to the Inspector General, a staggering 19,000 reports of this type of fraud were filed over a six-week period in 2012, and the office continues to receive an average of 50 reports each day. The U.S. Treasury's efforts to embrace electronic payments – both in the IRS and Social Security Administration – are clearly putting seniors in the crosshairs of cybercrime.

Moreover, elderly beneficiaries who still file taxes and receive debit card refunds face even more risk. Unlike paper checks, debit cards can be seized and used without sufficient identity verification. Thieves have already exploited this reality across the country by taking advantage of people who receive tax returns in the form of similar debit cards. Thieves can simply target senior citizens in their home by lifting the debit cards right from their mailboxes. Further, postal workers have even been targeted – and one was even murdered – by thieves seeking a mail truck full of debit cards and master keys to mailboxes at assisted living centers and apartment complexes.

The IRS Also Burdens Seniors by No Longer Sending Paper Tax Forms.

In addition to the cybersecurity risks that electronic tax-filing creates for seniors, the IRS electronic filing effort is also creating hardship for seniors who wish to file their taxes on paper. The IRS no longer mail tax forms to U.S. taxpayers. This policy overlooks the 30 million Americans who still file their tax returns by mail. While the new policy makes sense for taxpayers already filing electronic returns, citizens who don't have access to computers (45 percent of all seniors), or the skills to use them, face a challenge.

The IRS has said that the tax forms are available at many post offices and public libraries, yet Consumers for Paper Options receives complaints from seniors that this is not always true. We have talked with seniors who make repeated unsuccessful trips to these facilities in search of tax documents. The paperless policy also makes it difficult for citizens in rural areas who have no access to the Internet and are miles from nearby post offices and libraries.

The IRS should reverse its decision and continue to supply tax forms and instructions to senior citizens and others who need or want them. With the number of e-filers growing each year, the pool of paper filers will no doubt shrink with time. Until then, however, the federal government should not deny this important service to senior citizens and low-income individuals who cannot e-file, or to taxpayers with legitimate concerns about identity theft.

Conclusion: Electronic Tax-Filing Puts Seniors and Other Americans at Risk.

The simple truth is that the electronic tax-filing system is not secure, yet a primary goal of the IRS is to completely transition the American people to e-filing. As the experiences of millions of identity theft victims demonstrate, the IRS is not equipped for secure electronic tax-filing, and thieves are using this fact to their advantage.

The IRS policy of electronic tax-filing and direct-deposited refunds is empowering thieves to rob vulnerable citizens of their identities and forcing taxpayers to make up the difference.

Before the IRS takes further steps to encourage electronic filing and the direct deposit of returns, it must dramatically improve the safeguards in place to protect citizens from fraudulent behavior. In the meantime, it should not discourage paper-based tax filing, nor should it put roadblocks in place that discourage paper-based filings.

Consumers for Paper Options encourages this Committee to continue efforts to protect Americans from tax-related identity theft. You should insist that the IRS provide continued access for paper-filing and reinstate the mailing of paper tax forms – while the agency also works to secure the identity of law-abiding taxpayers who are being exposed to criminal fraud.

International Association of Jewish Genealogical Societies (IAJGS)
6052 Hackers Lane Agoura Hills, CA 91301
818-889-6616 tel 818-991-8400 fax
www.iajgs.org

STATEMENT FOR THE RECORD, SENATE COMMITTEE ON FINANCE WRITTEN COMMENTS ON PROVISIONS RELATING TO TAX FRAUD AND IDENTITY THEFT AND THE SOCIAL SECURITY ADMINISTRATION'S DEATH MASTER FILE, ALSO KNOWN COMMERCIALLY AS THE SOCIAL SECURITY DEATH INDEX.

I. INTRODUCTION:

The Senate Committee on Finance, held a Hearing on 16 April 2013 entitled:
"TAX FRAUD AND TAX ID THEFT: MOVING FORWARD WITH SOLUTIONS".
The public may submit statements within two weeks of the hearing and this statement fulfills that opportunity on behalf of the International Association of Jewish Genealogical Societies (IAJGS).

II. IAJGS BACKGROUND & CONTACT INFORMATION:

The International Association of Jewish Genealogical Societies is the umbrella organization of 72 Jewish genealogical societies and Jewish historical societies worldwide whose approximately 10,000 members are actively researching their Jewish roots. In 2013, we are holding our 33rd consecutive annual International Conference on Jewish Genealogy (www.iajgs.org). We want to ensure that our members will be allowed continued and maximum access to these vital records.

The IAJGS and its predecessor organization were formed in 1988 to provide a common voice for issues of significance to its members and to advance our genealogical avocation. One of our primary objectives is to promote public access to genealogically relevant records.

Contact Information:
IAJGS official mailing address is:
IAJGS
PO Box 3624
Cherry Hill, NJ 08034-0556

For purposes of this statement please use the following contact information:

Jan Meisels Allen,
Vice President, IAJGS
6052 Hackers Lane
Agoura Hills, CA 91301 (818) 889-6616 tell (818) 991-8400 fax (call before submitting a fax)
E-mail: vicepresident@iajgs.org

Officers
Michael Goldstein, Jerusalem, Israel, President@iajgs.org
Jan Meisels Allen, Agoura Hills, CA, USA, Vicepresident@iajgs.org
Joel Spector, Cherry Hill, NJ, USA, Secretary@iajgs.org
Paul Silverstone, New York, NY, USA, Treasurer@iajgs.org
Immediate Past President
Anne Feder Lee, Honolulu, HI, USA, Anne@iajgs.org

Directors-at-large
Nolan Altman, Oceanside, NY, USA, Nolan@iajgs.org
Daniel Horowitz, Kfar Saba, Israel, Daniel@iajgs.org
Kahlile Mehr, Bountiful, UT, USA, Kahlile@iajgs.org
Mark Nicholls, Edgeware Middlesex, UK Mark@iajgs.org
Jay Sage, Newton Center, MA, USA Jay@iajgs.org
Jackye Sullins, Carlsbad, CA, USA, Jackye@iajgs.org

Thank you for the opportunity to present the IAJGS concerns regarding the Committee's discussion on the reduction of public access to the commercial version of the Death Master File (DMF), the Social Security Death Index (SSDI). For the purposes of this statement, we will be addressing access to the SSDI rather than the DMF, as the SSDI is the version that genealogists are permitted to access.

We were disappointed that the genealogical community was not invited to participate at the April 16 hearing and hope that when bill-specific hearings affecting access to the DMF/SSDI are scheduled, forensic genealogists will be invited to testify. IAJGS suggests that you invite representatives from the Council for the Advancement of Forensic Genealogy [CAFG] [http://www.forensicgenealogists.com/index.html] to discuss why genealogists are an important stakeholder in the proposed legislation. The Association of Professional Genealogists (APG) includes on their website listings of specialties including "forensic" [http://www.apgen.org/directory/search.html?type=specialty&new_search=true] therefore, you may wish to invite them as well for a forensic genealogist.

It is ironic that a system that is used to prevent identity theft by permitting employers, financial organizations, insurance companies, pension funds, and others the ability to check names against those deceased as reported on the Death Master File, [http://www.ntis.gov/products/ssa-dmf.aspx] is now being considered—inappropriately—as an instrument of identity theft.

Included in Chairman Baucus's opening remarks were examples of living persons who have been victims of identity theft—a testament that the DMF/SSDI did NOT provide the information for their having their identity stolen and the ensuing nightmare that these individuals endured. Unfortunately, there are many such instances that have been documented—that living persons are victims of such a scourge. Denying access to genealogists to the DMF/SSDI will not prevent such occurrences.

We support the Committee's intent to protect the residents of the United States from improper usage of their personal information, and to protect them from identity theft. However, rarely has it been documented that an individual's identity is violated by access to vital records or the SSDI. Rather, the violations occur due to computer breaches from government and private enterprises. A 2009 study stated "in the last five years, approximately 500 million records containing personal identifying information of United States residents stored in government and corporate databases was [sic] either lost or stolen"[1]. Many of these computer breaches have been well documented in the press.[2]

Genealogical Community Positions on Access to the Social Security Death Index

While we advocate all genealogists should have immediate access to the SSDI, we would support the two year delay in access—and if necessary the third year—that National Taxpayer Advocate Nina Olson advocated during previous testimonies.

This support is with the caveat that certain genealogists are to be eligible for certification for immediate access. These genealogists include: forensic genealogists, heir researchers, and those researching individual genetically inherited diseases. Examples of those who need immediate access to the SSDI include:

- Genealogists who work in the field of forensic genealogy.

1. Helping the military in the repatriation of the remains of servicepersons lost in previous military conflicts by identifying and locating their living relatives.
2. Helping county coroners by identifying the relatives of unclaimed persons.

- Heir genealogists assist attorneys who need to find missing heirs to settle estate cases.
- Genealogists who are researching a genetically inherited disease in their family where time is of the essence in locating extended family members who may have

inherited a gene and need to be tested and treated as quickly as possible.

We recommend that those genealogists with government or legal contracts doing work as forensic genealogists or heir researchers and other certified or accredited genealogists be certified for immediate access. Genealogists who are already certified by the Board for Certification of Genealogists (BCG) or the International Commission for the Accreditation of Professional Genealogists (ICAP-GEN) should be immediately certified by the Department of Commerce—which is the government department mentioned responsible to certify in several bills addressing access to the DMF/SSDI.

Supporting Information for the Aforementioned Genealogical Community Position

- **Genealogists Are Not the Cause of Identity Theft.**

Thieves are the cause of identity theft. Financial institutions and government agencies have been hacked into numerous times and that has been documented [1, 2]. If we accept the continued use of computerized data, and the continued likelihood of hacking occurring to any given database at any time, then we must also accept that, occasionally, misuse of data will occur. It is not reasonable, Constitutional, or in the Nation's interests, to remove public documents from public access.

Removal of the SSDI from public access would not necessarily reduce the problem of fraudulent use of a Social Security number. As it will no longer be available as a reference check to many who use it as an identity theft deterrent, it may well increase identity theft.

For those whose deceased children whose Social Security numbers were fraudulently used and as parents and grandparents there is nothing that we can adequately express to parents of deceased children about their grief over the agonizing loss of their children. But there is no proof that they obtained the Social Security numbers from the DMF/SSDI rather than someone in an institution or office that had access to those numbers using them fraudulently. Unfortunately, medical identity theft, whereby medical employees have been found to steal patient's identification has become a growing business.[3]

For a real solution to this problem, see below "IRS Needs to be More Proactive."

- **Interest in Family History/Genealogy**

Millions of Americans are interested in their family history; The Harris Interactive Poll taken in March 2012, found that four in 5 Americans have an interest in learning about their family history. The 2011 Poll also reported 75% of Americans believe it is important to pass along their family's lineage to the next generation.[4] Genealogists doing U.S. research located both in and outside the United States rely on the Social Security Death Index.

- **Compassionate Genealogy**

This has several components:

Working with Coroners to Identify Deceased's Next of Kin

People are going to their graves with no family to claim them. Medical examiners and coroners' offices—frequently overstretched with burgeoning caseloads—need help in finding next of kin of the deceased. The deceased's identities are known; it's their next of kin that are unknown in these cases. Over 400 genealogists are now offering their volunteer services to help locate the next of kin for unclaimed persons. The identities of these people are known, but the government agencies are not

always able to find the families, so they are literally unclaimed. It is a national problem with which coroners must cope. See unclaimedpersons.org

Working with the Military

There are literally tens of thousands of United States Veterans' remains left unclaimed throughout the Nation. Sometimes decades pass while these remains are waiting to be identified as Veterans and given a proper military burial. Genealogists work with the military to locate relatives of soldiers who are still unaccounted for from past conflicts. By finding relatives, the military can identify soldiers using DNA, and notify the next of kin so the family can make burial decisions. While using DNA, the genealogists also need SSNs to help assure they are finding the correct person's family [5].

- **Family Medical History**

Genealogists use the Social Security Numbers (SSNs) to appropriately identify records of people when tracing **family medical history**, especially if the person has a common name: Sara Cohen, Tom Jones, Jose Martinez, Mary Smith etc. During a 2012 House Ways and Means Subcommittee hearing on Social Security , the representative of the Consumer Data Industry Association (CDIA), mentioned CDIA had conducted a study and found some people with common names, i.e. Smith, also had the same last four digits on their Social Security number, validating why the complete Social Security number is necessary.

Genealogy assists researchers in tracing family medical problems that are passed on from generation to generation. Information included in birth, marriage, and death records is critical to reconstructing families and tracing genetically inherited attributes in current family members. The SSN is essential to make certain that one is researching the correct person. Increasing numbers of physicians are requesting that their patients provide a "medical family tree" in order to more quickly identify conditions common within the family[6]. Information on three generations is the suggested minimum. The US Surgeon General includes preparing a family medical history as part of the American Family Health Initiative[7].

There are many genetically inherited diseases, but for the purposes of this statement, we will mention the *BRCAI* and *BRCA2* genes' mutations and breast and ovarian cancer. The following information is from the National Cancer Institute [8].

> "A woman's risk of developing breast and/or ovarian cancer is greatly increased if she inherits a deleterious (harmful) *BRCA1* or *BRCA2* mutation. Men with these mutations also have an increased risk of breast cancer. Both men and women who have harmful *BRCA1* or *BRCA2* mutations may be at increased risk of other cancers.
>
> The likelihood that a breast and/or ovarian cancer is associated with a harmful mutation in *BRCA1* or *BRCA2* is highest in families with a history of multiple cases of breast cancer, cases of both breast and ovarian cancer, one or more family members with two primary cancers (original tumors that develop at different sites in the body), or an Ashkenazi (Central and Eastern European) Jewish background.
>
> Regardless, women who have a relative with a harmful *BRCA1* or *BRCA2* mutation and women who appear to be at increased risk of breast and/or ovarian cancer because of

their ***family history*** [emphasis added] should consider genetic counseling to learn more about their potential risks and about *BRCA1* and *BRCA2* genetic tests.

The likelihood of a harmful mutation in *BRCA1* or *BRCA2* is increased with certain familial patterns of cancer [emphasis added]. These patterns include the following:

For women of Ashkenazi Jewish descent:

- any first-degree relative diagnosed with breast or ovarian cancer; and
- two second-degree relatives on the same side of the family diagnosed with breast or ovarian cancer. "

This form of breast cancer is something not unique to Ashkenazi Jews, as studies have demonstrated that this has also been found in the Hispanic communities in New Mexico and Colorado--who did not know they were descended from Sephardic Jews who had hidden their Jewish identity to survive the Inquisition in the 15th century. This is described in Jon Entine's *Abraham's Children: Race, Identity and the DNA of the Chosen People*, by the Smithsonian in their article, *The Secret Jews of San Luis Valley*, and *The Wandering Gene and the Indian Princess: Race, Religion, and DNA*[9]

People who have had members of their families diagnosed with breast cancer need to know whether past family members may have also died from this disease, in order to determine if it is inherited. Both current and future generations need to have this information in order to make decisions about whether to prophylactically remove both breasts and ovaries (which can mean the difference between early detection and treatment versus possible early death). This is something both men and women need to be able to research--as either can be carrying the gene mutation. The SSDI is a critical tool in assuring researchers that the records they have located on possible ancestors are indeed the correct persons, especially when they have a common name.

We use this as only one example of inherited diseases that require the ability to research ancestry using a SSN—regardless of ethnicity.

- **Genealogy as a Profession**

While there are millions of people who actively study and research their family history as an avocation, there are many others who earn their livelihoods as professional genealogists. Professional genealogists use the SSDI to (1) help track heirs to estates, (2) find title to real property, (3) find witnesses to wills that need to be proved, (4) work on the repatriation projects [see Working with the Military], (5) track works of art—including stolen art—and repatriation of looted art work during the Nazi era of World War II, and (6) assist in determining the status of Native American tribes and tribal members to prove—or disprove—that they are entitled to share in Tribal casino revenues.

- **IRS Needs to Be More Proactive**

If the IRS were to routinely run Social Security numbers included in tax returns against the death index, they might avoid giving refunds to deceased individuals.

"Operation Rainmaker" (also known as Operation TurboTax), was a tax fraud operation in the Tampa Bay area. Law enforcement interviews specified that the IRS, while cooperating with other law enforcement officers, is not authorized to share information with local law enforcement departments, hampering efforts to protect their citizens. It was mentioned during the April 16 hearing, that with the aggrieved party's permission, the IRS is now permitting sharing of information with law enforcement agencies. If the federal government is serious about addressing identity theft that uses a person's Social Security number, then the IRS needs to be given legislative authority to share information with local, county and state law enforcement organizations. It was also stated that filing tax refunds for under $10,000 will not get any attention. "Operation Rainmaker" found the average tax fraud was about $9,500, below the $10,000 threshold[10]. This is another practice that the Congress needs to review, as the criminals who are perpetrating this fraud know they will be undetected!

The IRS needs to amend their practice when the filing involves a deceased child, to require some verification to determine which is a valid filing. Today when a child is born in the United States an application is made for a Social Security number shortly after birth, and the SS-5 application has both parents' names included on the application. The IRS could do a name-match to determine if the parents filing for the refund on a deceased child were the same as those on the SS-5 application.

- **Support For Efforts to Cease Identity Theft**

- If income tax returns were electronically compared to the Master Death File, matching cases could be flagged for special processing, and the person attempting to create a tax fraud could be stopped before the fraud occurs.

- A parent's social security number should be required when filing a tax return for any minor. It is an extremely rare occurrence that a minor child would not be listed as a dependent on the parent or guardian's tax filing. If the minor dies, the IRS could have a procedure to flag any filings without the parent's social security number, again preventing the fraud. The *National Taxpayer Advocate's Report to Congress for 2012* specifically highlights the benefits of the IRS issued Identity Protection PINs and encourages that program expansion and timeliness of providing PINs to the victims of identity theft [11] and in its 2011 report suggested that taxpayers should be allowed to turn off their ability to file tax returns electronically. Any family that suffers a death could elect to turn off the electronic filing ability.

- Criminal penalty statutes for those who fraudulently use Social Security Numbers, including, but not restricted to, those who misuse their positions (*e.g.*, hospital, medical institution and office personnel, financial and credit card organizations personnel, prison corrections officer, college or university registrar etc.)

For the reasons stated above:

- genealogists are **NOT** the cause of identity theft;

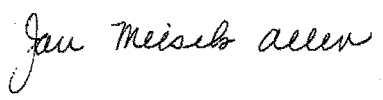
- genealogists have legitimate, professional and life-saving reasons to have immediate access to the SSDI; and

- proactive measures are needed to prevent identity theft and vigorously pursue and punish the **TRUE** identity thieves,

IAJGS respectfully encourages the Committee to continue the commercial version of the Death Master File, known as the Social Security Death Index, to be available to the public including the genealogical community.

On behalf of the International Association of Jewish Genealogical Societies we appreciate the opportunity to submit our comments, and for the occasion to bring to the Committee's attention the many services the genealogy community performs for local, **state and federal government offices.** We look forward to working with the Committee and staff to find an accommodation that provides forensic genealogists, heir researchers and those researching genetically inherited diseases with immediate access to the DMF/SSDI and others to have access within 2-3 years to the DMF/SSDI.

Respectfully submitted,



Jan Meisels Allen
IAJGS Vice President
Chairperson, IAJGS Public Records Access Monitoring Committee

---

[1] http://www.identitytheft.info/breaches09.aspx
[2] http://www.nctimes.com/news/local/article_3b98ce38-f048-597e-9a76-47321d114326.html
http://www.washingtonpost.com/politics/tricare-military-beneficiaries-being-informed-of-stolen-personal-data/2011/11/23/gIQAcRNHtN_story.html
Copes, H., and Vieraitis, L.M. (2009). Understanding identity theft: Offenders' accounts of their lives and crimes. *Criminal Justice Review*, *34*(3), 329-349
[3] http://consumerist.com/2010/03/id-theft-ring-used-hospital-records-for-300k-shopping-spree.html
[4] For complete survey methodologies, including weighting variables please contact mediarelations@ancestry.com and for the 2011 survey go to:
http://corporate.ancestry.com/press/press-releases/2012/01/ancestry.com-partners-with-historical-society-of-pennsylvania-to-bring-the-states-rich-history-online/
This survey was conducted online within the United States by Harris Interactive on behalf of Ancestry.com from March 13-15, 2012 among 2,211 adults ages 18 and older and from August 5-9, 2011 among 2,950 adults ages 18 and older.
[5] http://www.aarp.org/relationships/genealogy/info-06-2011/genealogy-tips.html
http://www.familiesforforgottenheroes.org/Genealogist.htm
[6] Mayo Clinic staff: "Medical History: Compiling your medical family tree," http://www.mayoclinic.com/health/medical-history/HQ01707;
[7] https://familyhistory.hhs.gov/fhh-web/home.action
[8] http://www.cancer.gov/cancertopics/factsheet/Risk/BRCA
[9] Abraham's Children: Race, Identity, and the DNA of the Chosen People. Jon Entine, Grand Central Publishing, New York, N.Y. 2007
http://www.smithsonianmag.com/science-nature/san-luis-valley.html
The Wandering Gene and the Indian Princess: Race, Religion, and DNA. Jeff Wheelwright. WW Norton & Co. New York, NY, 2012.
[10] http://www.youtube.com/watch?v=gpgTFO7nMBk
[11] http://www.irs.gov/pub/irs-pdf/p2104.pdf

STATEMENT FOR THE RECORD
OF
TODD DAVIS, CHIEF EXECUTIVE OFFICER OF
LIFELOCK INC.

BEFORE THE UNITED STATES SENATE COMMITTEE ON FINANCE

Hearing on Tax Fraud and Tax ID Theft: Moving Forward with Solutions

April 16, 2013

Chairman Baucus, Ranking Member Hatch, I thank you for this hearing and appreciate the opportunity to submit this statement for the record. As the leader in consumer risk management with patented analytics, proven expertise and real-time insight into consumer behavior, I am pleased to share with you LifeLock's perspectives on solutions to combat identity theft-related tax fraud. In short, LifeLock advocates the use of patented, predictive fraud analytics to reduce fraud upfront, incorporation of alerting and multi-factor authentication technology for victims of taxpayer identity theft combined with high levels of customer service to help stop fraud and provide taxpayers greater control over the use of their identity in future tax filings.

About LifeLock and ID Analytics

LifeLock and ID Analytics, a wholly-owned subsidiary of LifeLock, are recognized experts at the detection, analysis, and identity fraud protection in both the private and public sectors.

LifeLock is the industry leader in protecting individuals from identity theft and related fraud. In the sixth annual identity protection service scorecard by Javelin Strategy & Research[i], for example, LifeLock Ultimate™ was scored as first place overall by demonstrating across-the-board excellence in service quality and capabilities. Also recognized was the proactive nature of LifeLock Ultimate™, naming it Best in Detection. This proactive protection, which helps stop identity fraud before the damage is done, is a critical differentiator for LifeLock versus many alternative solutions that only notify consumers after an identity fraud has occurred.

ID Analytics, a LifeLock company, supports the identity risk management needs of over 250 leading companies to help stop fraud, authenticate individuals, minimize credit risk, and reduce financial losses. ID Analytics provides identity risk management services to eight of the top ten credit card issuers, six of the top ten financial services companies, three of the top four wireless carriers, nearly five million consumer subscribers and several government agencies.

LifeLock's and ID Analytics' integrated capabilities offer industry leading identity fraud detection and customer service for those who are victims of identity theft. These capabilities, combining predictive analytics and real-time alerts, pioneered in the financial services industry,

are also applicable to the problem of tax identity fraud that plagues the Internal Revenue Service as well as revenue agencies across the U.S.

Tax-Related Identity Theft

Identity thieves will fraudulently claim $21 billion in fraudulent tax refunds over the next five years, according to a 2012 report[ii] issued by the Inspector General for the U.S. Department of Treasury and the Internal Revenue Service Acting Commissioner Miller has testified that over two million suspicious returns have been suspended or rejected so far in the 2013 filing season. We know this problem is not unique to the IRS. We see private industries, especially those in the financial services and banking sectors, wrestle with the same problem. When aggregated, the private sector's exposure is greater than the IRS' challenges. For example, 12.6 million adults in the US, representing 5.26% of the adult population, were victims of identity fraud which generated $21 billion in total cost of identity fraud to consumers and enterprises in the U.S.[iii]

Apply Commercial Best Practices to Solve Tax Fraud and Identity Theft

In the 1990's, financial services companies pioneered the use of predictive analytics in their real-time operations in response to ever evolving types of fraud. More recently, customer service organizations, supporting millions of clients, implemented real-time messaging and alerts in order to provide customers greater control over the use of their identity, enhance customer service, and detect unauthorized transactions.

LifeLock and ID Analytics provide these very capabilities and solutions that can help stop fraud on the front end, provide a high level of customer service to victims of taxpayer identity theft, and engage taxpayers to help stop fraud in future tax filings.

We believe the same identity and fraud-related services provided to the world's largest companies can identify, detect, and reduce the same fraud that the Treasury Department must control and minimize. This process can include the use of alerting technology, similar to alerts sent by large institutions when a customer's profile or address has changed, to give the customer greater control over the use of their identity.

A flexible, multi-step risk-based approach, similar to what is common-place in private banking enterprises, will detect and reduce identity theft for revenue agencies, enabling delivery of legitimate tax-return refunds with more fraud detected at less expense and with less effort.

Returns that are scored as low-risk can be automatically approved for refunds while high-risk identities should be recommended for additional automated fraud screening or referred to answer a series of personalized, network-based authentication questions. This approach can be applied to millions of returns by operating as a funnel, leaving only a small subset of individuals who require additional verification, thus minimizing customer friction and costs to adjudicate or review a tax filing.

The rank ordering of risk is designed to handle high volumes of transactions and minimize the

amount of friction incurred by a customer while maximizing the enterprise's security and fraud detection. For revenue agencies, this translates into low false positive rates and the application of additional resources and money on the riskiest individuals. Using this approach, the majority of low-risk individuals are not subject to additional automated or manual reviews thereby improving their overall customer experience and minimizing a revenue agency's down-stream manual review costs.

As an optional next step, for those identities exceeding a revenue agency's risk threshold, automated review capabilities should be applied. These capabilities are transparent to the taxpayer and provide the agency a chance to review high-risk filings and learn of other attributes to help clarify potential risk. For example, ID Analytics offers the ability to identify how identity manipulators create and use improper aliases to commit fraud or avoid matching a "negative" or "do not pay" list.

In the third step, the IRS could apply review tools to test high-risk identities that cannot be resolved using automated tools. While there are a variety of manual review tools techniques available, the risk based approach strives to minimize their use as they tend to increase costs and typically require additional action by the customer.

Finally, for those individuals already victimized by taxpayer identity fraud, we recommend the use of a real-time alerting technology to connect registered victims with new taxpayer filings. ID Analytics built a real-time alerting platform to help stop identity misuse and has integrated it into LifeLock's proactive service offerings. Similar "monitoring and alerts" capabilities, managed by government officials, could help victims better manage their future tax filings and protect their identity in tax filing transactions that they did not initiate.

Conclusion

The IRS has worked diligently in recent years to curb identity theft and screen returns before processing. It is our hope that the Committee will provide the IRS with clear guidance, using the lessons learned and best practices available from leading financial enterprises and companies like LifeLock and ID Analytics, to help them incorporate existing, proven models of fraud detection into their processes. We stand ready to help both the IRS and the Committee better understand this dynamic marketplace and the solutions that have been most effective in identifying and stopping fraudulent transactions.

[i] (Source: Javelin Strategy & Research's 2012 Identity Theft Protection Services Scorecard, October 2012)
[ii] (http://www.treasury.gov/tigta/auditreports/2012reports/201242080fr.html)
[iii] (Javelin Strategy & Research (2013))

PRESIDENT: Rep. Charles Curtiss, TN
PRESIDENT-ELECT: Rep. Greg Wren, AL
VICE PRESIDENT: Sen. Neil Breslin, NY
SECRETARY: Sen. Travis Holdman, IN
TREASURER: Rep. Steve Riggs, KY

VIA E-MAIL

April 15, 2013

The Honorable Max Baucus
Chair, U.S. Senate Committee on Finance
219 Dirksen Senate Office Building
Washington, D.C. 200510

Dear Chairman Baucus:

As leaders of the National Conference of Insurance Legislators (NCOIL), we would like to commend you on your exploration of tax fraud in the 113th Congressional Session, evidenced by your upcoming hearing, "Tax Fraud and Tax ID Theft: Moving Forward with Solutions." We also would like to reaffirm for the record the very important state-mandated use of the Social Security Administration's Death Master File (DMF) as a consumer protection under the NCOIL *Model Unclaimed Life Insurance Benefits Act*. Since its adoption, the model has been enacted in six states, is now pending in five, and is being considered in numerous others.

As NCOIL related to Congress last year (letter attached), the NCOIL model relies on the DMF to help ensure that life insurance beneficiaries receive their promised benefits. The model act was developed in 2011 in response to growing concern that life insurance companies would not always use the DMF to find deceased life insurance policyholders for which life insurance death benefits were owed—but would commonly use tools like the DMF to identify deceased owners of annuity contracts to cease payments.

The NCOIL *Model Unclaimed Life Insurance Benefits Act* (1) compels routine identification of deceased policyholders by use of the DMF or no less comprehensive database, (2) establishes steps for beneficiary notification, (3) promotes timely payment of claims to beneficiaries, and (4) in the event that benefits go unclaimed, provides clear procedures for life insurers to escheat the funds, per unclaimed property laws.

Since adoption, this model in some form has been passed in Kentucky, Maryland, Montana, New Mexico, New York, and Alabama. Five states, including Massachusetts, Nevada, North Dakota, Rhode Island, and Vermont have legislation pending in 2013 legislative sessions, while yet others are considering the model.

We again appreciate the opportunity to bring our *Model Unclaimed Life Insurance Benefits Act* to your attention as Congress reviews DMF-related issues. NCOIL takes seriously concerns regarding release of personal information through the DMF and the need to protect against fraudulent activity. Also vitally important is making sure that companies follow through on their promises of payment—particularly to individuals who may have recently lost a loved one. We hope any federal legislation will acknowledge this.

NCOIL is an organization of state lawmakers whose main area of public policy concern is insurance legislation and regulation. Many legislators active in NCOIL either chair or are members of the committees responsible for insurance legislation in their respective state houses across the country.

For more information, please feel free to contact the NCOIL National Office at 518-687-0178.

Sincerely,

Rep. Charles Curtiss, TN
NCOIL President

Rep. George Keiser, ND
NCOIL President (2010-2011)

Rep. Robert Damron, KY
NCOIL President (2009-2010)

Enclosures

K/:NCOIL/2013 Documents/2007939C.doc

EXECUTIVE DIRECTOR: SUSAN F. NOLAN NATIONAL OFFICE: 385 JORDAN ROAD, TROY, NY 12180; TEL: 518-687-0178; FAX: 518-687-0401 WEBSITE: WWW.NCOIL.ORG
E-MAIL: INFO@NCOIL.ORG WASHINGTON OFFICE: 601 PENNSYLVANIA AVENUE, NW, SUITE 900, SOUTH BUILDING, WASHINGTON, DC 20004; TEL: 202-220-3014; FAX: 202-330-5004

NCOIL

National Conference of Insurance Legislators

...for the States

PRESIDENT: SEN. CARROLL LEAVELL, NM
PRESIDENT-ELECT: SEN. VI SIMPSON, IN
VICE PRESIDENT: REP. CHARLES CURTISS, TN
SECRETARY: REP. GREG WREN, AL
TREASURER: SEN. NEIL BRESLIN, NY

VIA E-MAIL

February 1, 2012

Representative Sam Johnson, Chair
U.S. House Committee on Ways & Means
Subcommittee on Social Security
1211 Longworth House Office Building
Washington, DC 20515

Dear Chairman Johnson:

As leaders of the National Conference of Insurance Legislators (NCOIL), we would like to update you regarding state insurance legislators' activity related to the Social Security Administration's Death Master File (DMF). We recently became aware of your February 2 hearing on the accuracy and uses of the DMF and thought that the Subcommittee should be cognizant of the NCOIL *Model Unclaimed Life Insurance Benefits Act* that relies on the DMF to help ensure that life insurance beneficiaries receive their promised benefits.

NCOIL Past President Rep. Robert Damron (KY) developed the model act in 2011 in response to insurance regulator, state treasurer, and media accounts that life insurance companies would commonly use tools such as the DMF to identify deceased owners of annuity contracts and cease annuity payments, but would not always use those same tools to find deceased life insurance policyholders, for which life insurance death benefits were owed. Rep. Damron believed that stronger company standards were needed to:

- compel routine identification of deceased policyholders
- establish steps for beneficiary notification
- promote timely payment of claims to beneficiaries

NCOIL believes that the model act—which is attached for your convenience—represents an important consumer protection as it serves to ensure the proper payment of policy benefits due to our constituents. NCOIL overwhelmingly adopted the model act following hours of research and debate from legislators across the country and with input from key interested parties.

The NCOIL model, as adopted, requires insurers to quarterly compare the DMF with holders of in-force life insurance policies and retained asset accounts. It calls for timely insurer efforts to confirm an insured or account holder's death, locate any beneficiaries, and provide them with claims forms and instructions. In the event that benefits go unclaimed, the model provides clear procedures for life insurers to notify state treasury departments and to escheat the funds, per unclaimed property laws. Several of the model's provisions, in fact, reflect the terms and business practices of a John Hancock Financial agreement with state treasurers regarding unclaimed life insurance benefits.

NCOIL takes seriously the statements in your hearing announcement regarding incorrect DMF death reports and a potential for identity theft. We agree that correcting false reports and protecting against ID fraud are critical policy goals. Also vitally important is making sure that companies follow through on their promises of payment—particularly to individuals who may have recently lost a loved one.

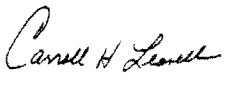
We appreciate the opportunity to bring our *Model Unclaimed Life Insurance Benefits Act* to your attention as you review DMF-related issues. NCOIL would welcome an opportunity to work with you to ensure that insurance companies continue to have access to important data in the DMF—while protecting against fraud and identity theft, the goal of H.R. 3475, the *Keeping IDs Safe Act of 2011.*

EXECUTIVE DIRECTOR: SUSAN F. NOLAN **NATIONAL OFFICE:** 385 JORDAN ROAD, TROY, NY 12180; TEL: 518-687-0176; FAX: 518-687-0401 **WEBSITE:** WWW.NCOIL.ORG
E-MAIL: INFO@NCOIL.ORG **WASHINGTON OFFICE:** 601 PENNSYLVANIA AVENUE, NW, SUITE 900, SOUTH BUILDING, WASHINGTON, DC 20004; TEL: 202-220-3014; FAX: 202-330-5004

NCOIL is an organization of state legislators whose main area of public policy concern is insurance legislation and regulation. Many legislators active in NCOIL either chair or are members of the committees responsible for insurance legislation in their respective state houses across the country.

For more information, please feel free to contact the NCOIL National Office at 518-687-0178 or our Washington, DC Office at 202-220-3014.

Sincerely,



Sen. Carroll Leavell, NM
NCOIL President

Rep. George Keiser, ND
NCOIL President (2010-2011)

Rep. Robert Damron, KY
NCOIL President (2009-2010)

Enclosures

K/NCOIL/2012/2007631

NCOIL
National Conference of Insurance Legislators
...for the states

PRESIDENT: SEN. CARROLL LEAVELL, NM
PRESIDENT-ELECT: SEN. VI SIMPSON, IN
VICE PRESIDENT: REP. CHARLES CURTISS, TN
SECRETARY: REP. GREG WREN, AL
TREASURER: SEN. NEIL BRESLIN, NY

Model Unclaimed Life Insurance Benefits Act

Adopted by the NCOIL Executive Committee on November 20, 2011, and by the Life Insurance & Financial Planning Committee on November 17, 2011. Amended and adopted by the Executive Committee on July 15, 2012, and by the Life Insurance & Financial Planning Committee on July 13, 2012. **Sponsored by Rep. Robert Damron (KY)**

Section 1. Short Title
This Act shall be known as the *Unclaimed Life Insurance Benefits Act.*

Section 2. Purpose
This Act shall require recognition of the escheat or unclaimed property statutes of the adopting state and require the complete and proper disclosure, transparency, and accountability relating to any method of payment for life insurance death benefits regulated by the state's insurance department.

Section 3. Definitions

A. "Death Master File" means the United States Social Security Administration's Death Master File or any other database or service that is at least as comprehensive as the United States Social Security Administration's Death Master File for determining that a person has reportedly died.

B. "Death Master File Match" means a search of the Death Master File that results in a match of the social security number or the name and date of birth of an insured, annuity owner, or retained asset account holder.

C. "Policy" means any policy or certificate of life insurance that provides a death benefit. The term "Policy" shall not include any policy or certificate of life insurance that provides a death benefit under an employee benefit plan (i) subject to The Employee Retirement Income Security Act of 1974 [29 USC 1002], as periodically amended, or (ii) under any Federal employee benefit program, or (iii) any policy or certificate of life insurance that is used to fund a preneed funeral contract or prearrangement, or (iv) any policy or certificate of credit life or accidental death insurance.

D. "Contract" means an annuity contract. The term "Contract" shall not include an annuity used to fund an employment-based retirement plan or program where the insurer is not committed by terms of the annuity contract to pay death benefits to the beneficiaries of specific plan participants.

Drafting note: All other terms used in this Act shall be interpreted in a manner consistent with the definitions used in [Insert State Insurance Code].

Section 4. Insurer Conduct

A. An insurer shall perform a comparison of its insureds' in-force life insurance policies and retained asset accounts against a Death Master File, on at least a semi-annual basis, to identify potential matches of its insureds. For those potential matches identified as a result of a Death Master File Match, the insurer shall:

1. within ninety (90) days of a Death Master File Match:

    a. complete a good faith effort, which shall be documented by the insurer, to confirm the death of the insured or retained asset account holder against other available records and information; and

EXECUTIVE DIRECTOR: SUSAN F. NOLAN NATIONAL OFFICE: 385 JORDAN ROAD, TROY, NY 12180; TEL: 518-687-0176; FAX: 518-687-0401 WEBSITE: WWW.NCOIL.ORG
E-MAIL: INFO@NCOIL.ORG WASHINGTON OFFICE: 601 PENNSYLVANIA AVENUE, NW, SUITE 900, SOUTH BUILDING, WASHINGTON, DC 20004; TEL: 202-220-3014; FAX: 202-330-3004

b. determine whether benefits are due in accordance with the applicable policy or contract; and if benefits are due in accordance with the applicable policy or contract:

i. use good faith efforts, which shall be documented by the insurer, to locate the beneficiary or beneficiaries; and

ii. provide the appropriate claims forms or instructions to the beneficiary or beneficiaries to make a claim including the need to provide an official death certificate, if applicable under the policy or contract.

2. With respect to group life insurance, insurers are required to confirm the possible death of an insured when the insurers maintain at least the following information of those covered under a policy or certificate: (1) Social Security number or name and date of birth, and (2) beneficiary designation information, (3) coverage eligibility, (4) benefit amount, and (5) premium payment status.

3. To the extent permitted by law, the insurer may disclose minimum necessary personal information about the insured or beneficiary to a person who the insurer reasonably believes may be able to assist the insurer locate the beneficiary or a person otherwise entitled to payment of the claims proceeds.

B. An insurer or its service provider shall not charge insureds, account holders, or beneficiaries for any fees or costs associated with a search or verification conducted pursuant to this section.

C. The benefits from a life insurance policy or a retained asset account, plus any applicable accrued interest shall first be payable to the designated beneficiaries or owners and in the event said beneficiaries or owners can not be found, shall escheat to the state as unclaimed property pursuant to *[Cite state statute for escheat or unclaimed life insurance benefits].*

Drafting note: Some states' insurance commissioners may want to develop an informational notice that apprises beneficiaries of their rights to the payment of interest on the benefits or proceeds of a life insurance policy or retained asset account. The written notice should be provided by a life insurer to a beneficiary prior to or concurrent with the payment of any life insurance proceeds or the settlement of any life insurance claim, where applicable.

D. An insurer shall notify the *[Insert the state agency for unclaimed property]* upon the expiration of the statutory time period for escheat that:

1. a life insurance policy beneficiary or retained asset account holder has not submitted a claim with the insurer; and

2. the insurer has complied with subsection A of this Section and has been unable, after good faith efforts documented by the insurer, to contact the retained asset account holder, beneficiary or beneficiaries.

E. Upon such notice, an insurer shall immediately submit the unclaimed life insurance benefits or unclaimed retained asset accounts, plus any applicable accrued interest, to the *[Insert the state agency for unclaimed property].*

Section 5. Unfair Trade Practices

Failure to meet any requirement of this Act is a violation of *[Insert State Unfair Trade Practices Statute].*

Drafting note: Some states' Unfair Trade Practices statutes specify that an act must be shown to be a "pattern" or "general business practice" in order to constitute a violation of that statute. In those instances, care should be taken in the adoption of this model to ensure consistency across those two statutes.

Section 6. Effective Date
This Act shall take effect on or after *[insert appropriate date]*.

Drafting note: Due to the fact that the provisions of this Act may necessitate significant changes to insurer compliance programs, states should consider up to a one-year delayed effective date.

Drafting note: To address other concerns with transparency and accountability in life insurer procedures relating to treatment of retained asset accounts, please refer to the NCOIL Beneficiaries' Bill of Rights, which requires extensive written disclosures to consumers and insurer reporting.

© National Conference of Insurance Legislators (NCOIL)

The U.S Senate

Committee on Finance

Records Preservation & Access Committee
Federation of Genealogical Societies, National Genealogical Society,
International Association of Jewish Genealogical Societies

P.O. Box 200940
Austin TX 78720-0940

Statement for the Record

Tax Fraud and Tax ID Theft: Moving Forward with Solutions

Submitted by

Frederick E. Moss, JD, LL.M.
access@fgs.org
972-679-5377

April 16, 2013

Chairman Baucus, Ranking Member Hatch, and distinguished Members of the Subcommittee:

Thank you for the invitation to submit this Statement for the Record on behalf of the genealogical community through its Records Preservation and Access Committee to supplement the record of the hearing held by the Committee on the 16th of April 2013.

I serve as the legal advisor to the Federation of Genealogical Societies and as a member of the Records Preservation and Access Committee more fully described below.

Be assured that the genealogical community shares the objective of protecting Americans against fraud and of addressing deficiencies in the current operation of the Social Security Administration's Death Master File. This hearing marks a valuable opportunity to express our views to Congress on this important subject and we commend the committee for continuing to monitor progress in addressing challenges faced by the Internal Revenue Service in confronting tax fraud by identity thieves.

Much Has Changed Since 2011

In the spring of 2011 we were all outraged by reports that identity thieves were filing fraudulent tax refund claims using the social security numbers (SSNs) of recently deceased children and adults. The comprehensive hearing held by the Subcommittee on Fiscal Responsibility and Economic Growth of this Senate Finance Committee on May 25, 2011 suggested that thieves had discovered vulnerabilities in our system for processing the online filing of tax returns and that we were seeing the leading edge of a flood of fraudulent refund claims for which we were ill-prepared. http://www.finance.senate.gov/hearings/hearing/?id=32a4f2cc-5056-a032-5258-8967bf140b37%2520

It was clear that refund checks were being mailed with a minimum of scrutiny and before the IRS would have received informational returns (W2s, 1099s, etc) that could verify the legitimacy of the refund claims.

Changes on Genealogical Websites

During the fall of 2011 some suggested that identity thieves could have gotten the SSNs of recently deceased children by online access to the Social Security Death Index (the commercial version of the Social Security Administration's Death Master File (DMF)). If thieves were using the SSDI, the IRS clearly was not. The SSDI, originally created as a fraud prevention resource, listed the SSNs of deceased persons and essentially "burned" the SSNs of those appearing thereon. It has been made widely available since the early 1980s and has been found to be a rich resource for a wide variety of legitimate users including medical researchers and genealogists.

As the tax filing season opened in early 2011, the SSDI was freely accessible by the general public from a number of web sites, to include most of the major sites serving the genealogical community without requiring a subscription or login. Several Senators, including members of this committee, voiced their concerns in a December 1, 2011 letter addressed to the CEO of Ancestry.com Inc and asked that they and other genealogical sites remove SSNs from their posting of the SSDI. http://www.brown.senate.gov/newsroom/press/release/after-call-from-sen-brown-ancestrycom-removes-social-security-numbers-from-website-to-prevent-fraud

Ancestry.com and other genealogical web sites immediately took measures designed to prevent the abuse of their resources by thieves. In addition to putting this data behind their subscription pay wall, Ancestry chose to conceal the SSN of the deceased for a period of time, even for their subscribers. Other genealogical sites took similar measures.
http://www.abc2news.com/dpp/news/local_news/investigations/website-stops-displaying-social-security-numbers-for-recently-dead

Efforts By the Internal Revenue Service

The information provided by the witnesses in this hearing give multiple reasons to be encouraged by the actions being taken to combat refund fraud and help victims of identity theft. Their written statements are available at:
http://www.finance.senate.gov/hearings/hearing/?id=62739085-5056-a032-5281-4500bf4d4fb3
The testimony of Steven T. Miller, Acting Commissioner of the Internal Revenue Service described a number of significant steps they have taken.

IRS Improved Filtering

We implemented new identity theft screening filters to improve our ability to spot false returns before we process them and issue refunds. For example, we designed and launched new filters that flag returns if certain characteristics are detected. While the development of effective filters is complex given the dynamic lives of legitimate taxpayers, these filters enable us to identify fraudulent returns even where a taxpayer's information has not been previously used for filing by an identity thief. These new filters specific to identity theft built on our overall refund fraud detection program, which already identified a significant number of identity theft cases besides those identified by the new filters. We have added even more identity theft filters for the 2013 filing season, including filters that target multiple refunds into a single bank account or to a single address. Page 3.

Expanded Criminal Investigations

Investigations of tax fraud related to identity theft have increased significantly over the past three fiscal years. In FY 2012, CI initiated 900 investigations involving identity theft, which is

more than triple the number of investigations in FY 2011. Indictments in identity-theft related cases also increased significantly, totaling nearly 500 in FY 2012, with 223 individuals sentenced and an average time to be served of 48 months. This compares with 165 indictments, 80 individuals sentenced, and a 44-month average sentence in FY 2011. Additionally, the direct investigative time spent by CI on identity theft cases has increased by 129 per cent in FY 2012 over FY 2011.

This trend is continuing in FY 2013. Already through April 9, 2013, more than 800 criminal identity theft investigations have been opened. Indictments in identity theft-related cases total 607, with 197 individuals sentenced and an average time to be served of 44 months.

In collaboration with the Department of Justice's Tax Division (DOJ-Tax) and local U.S. Attorneys' offices, the IRS conducted a highly successful coordinated identity theft enforcement sweep in January 2013. This nationwide effort against 389 identity theft suspects led to 734 enforcement actions, including 189 indictments, informations and complaints, and 109 arrests. Around the time of the sweep, IRS auditors and investigators conducted compliance visits to 197 money service businesses in a variety of locations across the country to help ensure that these businesses were not facilitating refund fraud and identity theft. Page 7.

Appropriate prosecution and sentencing of those perpetrating tax fraud related to identity theft has the potential of not only thwarting their predations but should serve as a deterrent to others tempted to follow their example. This begins to look like progress.

Thieves Have Moved On

As genealogical sites have protected SSNs of recently deceased people and the IRS has improved their filters used before refunds are paid, the possibility that thieves are exploiting information from the SSDI has dramatically diminished. It is likely that the SSDI was never the primary source of SSNs exploited by thieves. To the extent that it may ever have been used, the thieves have moved on. The list of those recently sentenced as reported on page 9 of Acting Commissioner Miller's Statement in this hearing indicates that the SSNs were (1) stolen from a community college's financial aid office, (2) stolen or tricks used to secure taxpayer's personal information, (3) involved residents of Puerto Rico, (4) stolen from a medical center records office, or (5) by breaking into a tax preparation office. Although an additional case involving the misuse of an online database was cited, that misconduct turned out to be by a "trusted user" of a commercially available non-genealogical database. It is significant that all three recent cases of tax fraud identity theft mentioned during the April 16 hearing involved <u>living</u> victims, not any who's SSNs might ever have been available on the SSDI.

National Taxpayer Advocate – "The Larger Question"

The written statement of National Taxpayer Advocate Nina E. Olson suggests a number of steps that would improve the IRS's ability to combat fraud and provide

better service to taxpayers. Page 16 of her statement includes the following major recommendation:

IV. To Reduce Taxpayer Burden and Cut Down on Tax Fraud, the IRS Should Be Empowered to Process Information Reporting Documents Like Forms W-2 Before Processing Tax Returns and Issuing Refunds.

She further observed that: ". . . [a]pproximately 97 percent of taxpayers receive at least one information return. Traditionally, the IRS has not matched this data with the items reported on the taxpayers' tax returns until long after the filing season. In 2010, the IRS closed 4.3 million cases in which it identified a discrepancy between the taxpayer's return and third-party information, leading to $7.2 billion in additional assessments."

In her testimony before this Senate Finance Committee hearing, she posed "the larger question" in suggesting that we need to begin considering whether the IRS should wait to begin paying refunds until after the close of the filing season. Found at 1:51:20 of the committee video at: http://www.finance.senate.gov/hearings/hearing/?id=62739085-5056-a032-5281-4500bf4d4fb3

Previous Statements Submitted in Related Hearing Last Session

Organizations representing the genealogical community have been actively monitoring these issues for the last year and, where the opportunity was provided, have sought to provide appropriate input. The Subcommittee on Fiscal Responsibility and Economic Growth of this Senate Finance Committee held the second in a series of hearings on Tax Fraud by Identity Theft on March 20, 2012. http://www.finance.senate.gov/hearings/hearing/?id=8c908260-5056-a032-525c-4f663b8d35f8%2520

Although we had not been asked to testify, the organizations sponsoring the Records Preservation and Access Committee did respond to the invitation to submit Statements for the Record of the March 20, 2012 Hearing on behalf of RPAC, FGS, NGS and IAJGS. **http://www.fgs.org/rpac/2012/04/02/ssdi-statement-for-the-record-senate-finance-subcommittee-hearing-20-march-2012/**

Addressing legislative proposals pending last spring, their recommendations to the Congress and to the genealogical community reflected the following coordinated position:

> While we advocate all genealogists should have immediate access to the SSDI, we would support the two year delay in access as proposed in S 1534-and if necessary the third year that National Taxpayer Advocate Nina Olson advocated during her oral testimony during the March 20th hearing. This support is with the caveat that certain genealogists are to be eligible for certification for immediate access. These genealogists include: forensic genealogists, heir researchers, and those researching individual genetically inherited diseases.

Although the legislative proposals pending before the Congress may have changed, the interests we then sought to protect have not.

This is not the statement I anticipated preparing for this hearing. I fully expected to be focused upon defining the categories of genealogists needing immediate access having conceded the appropriateness of a statute mandating a two or three year delay in access to SSDI data for the general public. A review of the steps already taken by the IRS and genealogical entities hosting SSDI data on their websites lead me to conclude that these measures have likely already achieved the benefits sought by such legislation.

I certainly know of no principled rationale that would support an embargo of SSDI data (including the "burned" SSNs) in excess of the three years cited as possibly required by the IRS to resolve estate issues. I understand this position to be consistent with that taken by the National Taxpayer Advocate.

Interests of the Genealogical Community

The interests of the genealogical community are not hard to understand. Access to records or the lack thereof, is the pivotal issue for genealogists. Without documentation, our family histories are more legend than history. Recent genetic advances have given additional significance to well-documented medical family histories. You can expect to hear expressions of concern from across the genealogical community whenever they may have reason to believe their access to these records is being threatened.

About the Records Preservation and Access Committee

The genealogical community works together through The Records Preservation and Access Committee (RPAC), a joint committee which today includes The National Genealogical Society (NGS), the Federation of Genealogical Societies (FGS) and the International Association of Jewish Genealogical Societies (IAJGS) as sponsoring members. The Association of Professional Genealogists (APG), the Board for Certification of Genealogists (BCG), the American Society of Genealogists (ASG), and the International Commission for the Accreditation of Professional Genealogists (ICAPGen) and industry representatives also serve as participating members. RPAC meets monthly, and more often if needed, to advise the genealogical and historical communities, as well as other interested parties, on ensuring proper access to vital records, and on supporting strong records preservation policies and practices.

Conclusion

Of the multiple congressional hearings addressing the threat of tax fraud by identity theft, this is the first to suggest that real progress is being made. By targeting the

criminal through the use of appropriate filters, investigation and aggressive enforcement, the efforts of identity thieves are being thwarted. Hopefully, by publicizing the results of successful prosecutions and the award of substantial penalties to the offenders, others may be deterred.

To the extent that the SSDI on genealogical websites was ever the source of compromised SSNs then used to file fraudulent tax refund claims, the responsible actions taken by those websites should have denied access to that information. In fact, while it is only informed speculation on my part that we should have seen few, if any, fraudulent returns attributable to SSNs accessed from the SSDI during the filing season just ended, the IRS should eventually be able to statistically confirm that that vulnerability targeting the deceased has been closed.

We should continue to be concerned that the SSNs of living persons will continue to be vulnerable so long as the IRS is mandated to expedite the payment of refund claims before they have even received information returns necessary to determine their validity.

The genealogical community has noticed that the only users of the SSDI for legitimate purposes called to testify in any of the congressional hearings addressing this issue have been from the financial/fraud prevention communities. Genealogists, medical researchers, those working with coroners and the Department of Defense to connect families with remains, have not been invited to appear. Pending legislative proposals (and the Administration's budget proposals) seem to lend credence to the relatively modern cliché that "if you aren't at the table, you are on the menu! "

Summary

We offer three main points:

(1) Our strongest message is that steps already taken by the IRS and genealogical entities to protect SSNs listed in the SSDI may have already intercepted this particular form of identity theft without waiting for any additional legislation.

(2) The SSNs of living people will remain vulnerable as long as the IRS mandate is to rush payments of tax refunds before information returns can be compared with the submitted return to assure its validity.

(3) As existing policy regarding public access to the Death Master File is reviewed, we urge that input from actual genealogists be sought. The members of the Records Preservation and Access Committee stand ready to assist in arranging for that input to both the Executive and Legislative branches. We can best be reached at access@fgs.org .

Links & Resources

(1) RPAC SFC 20 March 2012
http://www.fgs.org/rpac/2012/04/02/ssdi-statement-for-the-record-senate-finance-subcommittee-hearing-20-march-2012/

(2) SFC 25 May 2011
http://www.finance.senate.gov/hearings/hearing/?id=32a4f2cc-5056-a032-5258-8967bf140b37%2520

(3) Nelson Letter
http://www.abc2news.com/dpp/news/local_news/investigations/website-stops-displaying-social-security-numbers-for-recently-dead

http://genealogy.about.com/b/2011/12/16/genealogy-sites-pressured-into-removing-ssdi.htm

http://www.abc2news.com/dpp/news/local_news/investigations/website-stops-displaying-social-security-numbers-for-recently-dead

(4) SFC 16 April
http://www.finance.senate.gov/hearings/hearing/?id=62739085-5056-a032-5281-4500bf4d4fb3

(5) SFC 20 Mar 2012
http://www.finance.senate.gov/hearings/hearing/?id=8c908260-5056-a032-525c-4f663b8d35f8%2520

KENNETH H. RYESKY, ESQ., STATEMENT FOR THE RECORD, SENATE HEARINGS:

COMMITTEE ON FINANCE: "TAX FRAUD AND TAX ID THEFT: MOVING FORWARD WITH SOLUTIONS," 16 APRIL 2013.

SPECIAL COMMITTEE ON AGING: TAX-RELATED IDENTITY THEFT: AN EPIDEMIC FACING SENIORS AND TAXPAYERS," 10 APRIL 2013

I. INTRODUCTION:

The foregoing Committee hearings, covering similar issues, were held. This Commentary is accordingly submitted to the respective Committees.

II. COMMENTATOR'S BACKGROUND & CONTACT INFORMATION:

Background: The Commentator, Kenneth H. Ryesky, Esq., is a member of the Bars of New York, New Jersey and Pennsylvania, and is an Adjunct Assistant Professor, Department of Accounting and Information Systems, Queens College of the City University of New York, where he teaches Business Law courses and Taxation courses. Prior to entering into the private practice of law, Mr. Ryesky served as an Attorney with the Internal Revenue Service ("IRS"), Manhattan District. In addition to his law degree, Mr. Ryesky holds BBA and MBA degrees in Management, and a MLS degree. He has authored several scholarly articles and commentaries on taxation, including some submissions to various Congressional Committees.

Mr. Ryesky also engages in genealogical research on a personal and sometime professional basis. He is a member of the Jewish Genealogical Society of New York, and slated as a session panelist at the IAJGS Conference on Jewish Genealogy in Boston this coming August.

Contact Information: Kenneth H. Ryesky, Esq., Department of Accounting & Information Systems, 215 Powdermaker Hall, Queens College CUNY, 65-30 Kissena Boulevard, Flushing, NY 11367. Telephone 718/997-5070; E-mail: khresq@sprintmail.com.

Disclaimer: Notwithstanding various consultations between the Commentator and other interested individuals and organizations, this Commentary reflects the Commentator's personal views, is not written or submitted on behalf of any other person or entity, and does not necessarily represent the official position of any person, entity, organization or institution with which the Commentator is or has been associated, employed or retained.

III. COMMENTARY ON THE ISSUES:

A. Prior Commentaries Submitted:

The Commentator's previous relevant submissions to Congressional hearings include the following:

1. *Hearing on Identity Theft and Tax Fraud*, House Oversight & Government Reform Committee, Subcommittee on Government Organization, Efficiency, and Financial Management, 112th Congress, 2nd Session, November 29, 2012,<http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg77479/pdf/CHRG-112hhrg77479.pdf> .

2. *Joint Hearing on Social Security Numbers on Medicare Cards*, House Ways and Means Committee, Subcommittees on Social Security and on Health, 112th Congress, 2nd Session, August 1, 2012, <https://docs.google.com/file/d/0B0erD-E9YY0rS3BFZEtpSXhoWlU/edit>.

3. *Hearing on Tax Fraud involving Identity Theft*, House Ways and Means Committee, Subcommittees on Oversight and Social Security, U.S. House of Representatives,112th Congress, 2nd Session, May 8, 2012 <http://waysandmeans.house.gov/UploadedFiles/SFR_KennethRyesky_OS_SS_5_8_12.pdf>, *also available at* 2012 TNT 95-49.

4. *Hearing on Social Security Administration's Death Master File*, House Ways and Means Committee, Subcommittee on Social Security, U.S. House of Representatives,112th Congress, 2nd Session, February 2, 2012, <http://waysandmeans.house.gov/UploadedFiles/SFR_KennethRyesky_SS_2_2_12.pdf>, *also available at* 2012 TNT 25-32.

5. *Hearing on Tax Fraud by Identity Theft, Part 2: Status, Progress, and Potential Solutions*, Senate Committee on Finance Subcommittee on Fiscal Responsibility & Economic Growth, 112th Congress, 2nd Session, March 20, 2012, <http://www.gpo.gov/fdsys/pkg/CHRG-112shrg78502/pdf/CHRG-112shrg78502.pdf>, *also available at* 2012 TNT 56-30.

The foregoing commentaries are incorporated by reference, and now reasserted.

B. Points to be Emphasized:

Having reasserted his prior commentaries, the Commentator now stresses and emphasizes the following matters for the Committees:

1. The tax refund identity theft fraud victims showcased at the respective hearings were Ms. Hossli (witness), Mr. Saile (Mr. Baucus's constituent), and Mr. Hatch's two

Finance Committee staff members. It is noted that each of these is a living person, whose Social Security Number (SSN) and other personal data was not and could not have been obtained by the identity thieves from the Death Master File (DMF).

2. Ms. Olson's written statement, on page 16, confirms that "Approximately 97 percent of taxpayers receive at least one information return. Traditionally, the IRS has not matched this data with the items reported on the taxpayers' tax returns until long after the filing season." This spotlights a major flaw in the system, which the identity thieves have exploited.

3. The Form SS-5 Application for a Social Security Number specifically requires, for applications with respect to a child under 18 years of age, that the parents' names and SSNs be entered. The information necessary to screen tax returns to prevent an identity thief from fraudulently claiming someone else's deceased child as a dependent has accordingly long been available, but has not been used.

4. The Committees' attention is directed to the case of United States v. Alan N. Scott, 270 F.3d 30 (1st Cir. 2001) . The first two sentences of the third paragraph of the judicial opinion read,

> " In a 1998 case, a jury convicted Scott of conspiring to make and of making false claims to an agency of the United States, 18 U.S.C. §§ 286, 287 (1994). Scott filed twenty false income tax returns with the IRS for the tax year 1996 seeking tax refunds in the names of at least twelve people. "

Once Scott's conviction was obtained in 1998, the IRS could no longer deny knowing that stolen identity tax fraud was a problem. And by the time Tonya Ferguson pled guilty to stolen identity tax fraud in November of 2001 [United States v. Ferguson, No. 2:01-cr-20213-BBD, Western District of Tennessee], the day had long passed when the IRS could in good faith claim that Mr. Scott's stolen identity tax fraud scheme was an isolated aberrational fluke.

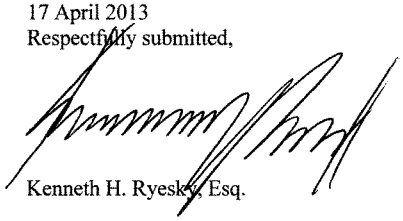
5. IRS Memorandum SBSE-04-1212-055 "Interim Guidance on Processing Identity Theft Cases" (20 December 2012) [www.irs.gov/pub/foia/ig/spder/SBSE-04-1212-055.pdf] has a control number reflecting origin in the IRS's Small Business / Self-Employed Division and not the Wage & Investment Division. This suggests that identity thieves may already be using business tax identification numbers (TINs) and committing tax return identity theft against businesses in addition to stealing the identities of individuals.

IV. CONCLUSION:

In prior Congressional hearings, the blame assignment agendas of many seem to have targeted the availability of the DMF, and, perhaps, the genealogy community. It has become increasingly clear that the total lockdown of the DMF would not and cannot stop stolen identity tax fraud, inasmuch as there numerous other sources for SSNs of individuals, living and dead.

The genealogy community as a whole understands the need to control identity theft, whether in connection with tax returns or otherwise, and could support a 2-year embargo on the release of entries in the DMF, provided that (A) genealogists be eligible for certification for early disclosure for purposes such as tracking lost heirs, investigating family medical histories, repatriating the remains of deceased individuals to surviving relatives, and other compelling purposes; and (B) the IRS takes a more positive and proactive role in screening and filtering the tax returns it processes before issuing refunds, including screening for multiple refunds to the same address and/or bank account.

17 April 2013
Respectfully submitted,



Kenneth H. Ryesky, Esq.

VISA

STATEMENT FOR THE RECORD

THE UNITED STATES SENATE COMMITTEE ON FINANCE

Hearing on Tax Fraud and Tax ID Theft: Moving Forward with Solutions

April 16, 2013

VISA Inc.
P.O. Box 8999
San Francisco, CA 94128-8999

ABOUT VISA: Visa Inc. is the world's largest retail electronic payments network. Visa has partnered with Federal and State Governments for over 20 years in developing and delivering innovative payment solutions that increase efficiencies, significantly reduce costs, and improve recipient payment/purchase experiences. The Visa Prepaid Debit card is currently offered through 80 government disbursement programs across 39 states in partnership with major financial institutions.

ELECTRONIC DISBURSEMENTS: STATES LEAD THE WAY FOR BENEFIT PAYMENTS AND TAX REFUNDS USING PREPAID CARDS

BACKGROUND: Effective March 2013, the U.S. Government requires all federal benefit payments to be made electronically. This switch has enormous benefits: immediate administrative savings; financial inclusion for the unbanked and underserved; accountability; and increased security. While this is good news, two facts remain: *federal tax refunds are excluded from the electronic payment requirement* and the federal government is not consistent in the application of electronic payments, resulting in the Internal Revenue Service printing and mailing 45 million paper tax refund checks annually. Not only does this approach eliminate opportunities to include the unbanked in the financial mainstream, it ignores industry and consumer trends. Government agencies across the US and around the world have long recognized that prepaid cards represent a cost effective way to make electronic payments to unbanked and underserved constituents who can benefit from their use every day.

THE DISBURSEMENTS. At the federal level, beginning in 2010, the US Treasury mandated the electronic disbursement of all benefit payments (Social Security, SSI, VA benefits, Federal Retirement, for instance). As the attached graphics show, states continue to lead the way on the use of prepaid cards. Today, 49 of 50 states have implemented card-based electronic payment programs for their constituents across a wide range of government disbursement programs: Child Support (48 states); Unemployment Insurance (44 states); Temporary Assistance for Needy Families (TANF); Emergency Disaster Relief; Workers' Compensation; Adoption Assistance; Foster Care; and Housing Subsidies for Beneficiaries and Property Owners. Additionally, 10 states are now issuing state income and property tax refunds via electronic means:

- Alabama	- Connecticut
- Georgia	- Illinois
- Louisiana	- Missouri
- New York	- Oklahoma
- South Carolina	- Virginia

SAVINGS TO TAXPAYERS AND INDIVIDUALS. The federal government estimates that switching social security benefits to electronic delivery will save U.S taxpayers $1 billion over ten years. This is because the cost of disbursing funds by paper checks is substantial: $1.03 per paper check compared to $.10 for an electronic payment. At the state level, the savings are equally significant. In one Midwestern state, the state saved more than $32 million over a 3 year period by switching to electronic disbursement. In Nebraska, the state reported it cost $.59 to issue a child support payment via paper check; switching to prepaid cards, the state reduced its costs to $.01 per payment, saving more than $368,000 per year.

ACCESS FOR THE UNBANKED AND UNDERSERVED. For the approximately 80 million US households who are unbanked and/or underserved, electronic payments increase access, reduce out of pocket costs, and provide additional security. Consider this: benefit check cashing fees can range from a flat fee of $3.00 to 2%- 6% of the face value of the check—hardly a fee the unbanked or underserved can afford. Using prepaid cards, this population gains access to the financial mainstream. Additional benefits include having faster access to their payments and

better security when comparing prepaid cards to paper checks. In one year alone, more than 540,000 Social Security and Supplemental Security Income paper checks were reported lost or stolen and had to be replaced, creating a financial hardship for the recipient and additional costs to the government.

THE BENEFITS. In addition to immediate savings, prepaid cards offer other significant benefits:

- ✓ *Money Management and Control.* Prepaid cards offer individuals greater access to, and control over their money. Cardholders spend only the funds loaded on the card. Government programs have visibility into potential unauthorized expenditures (TANFP, for instance).
- ✓ *Convenience.* Individuals have *immediate* access to their funds, faster transactions, and the ability to make purchases and pay bills in stores and on line while eliminating check cashing fees.
- ✓ *Acceptance.* Individuals can use their prepaid cards to make purchases at the millions of merchants who accepts cards–in stores, on-line or by phone. Additionally, there are more than a million ATMs worldwide that provide easy access to funds.
- ✓ *Additional Security.* According to the Government Accountability Office (GAO), there were 641,690 incidents of identity theft involving tax fraud in 2011. This number is on the rise and remains a top priority for IRS Criminal Investigators. Once a check is issued, there is no pulling it back if fraud is subsequently detected. With electronic payments, funds can be recalled.
- ✓ *Multiple Products and Solutions.* There is not a one size fits all approach with prepaid cards. Products are easily designed and delivered based on customer and consumer requirements: reloadable prepaid cards allow funds to be added at any time; partial authorization lets account holders split payments; and "zero" liability protections ensure consumers are not responsible for unauthorized charges. This is just a small sample of how products can be tailored to meet the specific requirements of federal programs.

THE FUTURE THROUGH ENHANCEMENTS AND INNOVATIONS. Industry continues to pave the way with significant innovations in technology. There are multiple products available, supported by technology enhancements and sophisticated risk and fraud prevention. Efforts are underway to test new technologies that allow multiple payments to be disbursed on the same card. Significant work is also being done on the fraud prevention front –not just in detecting fraud once the benefit has been issued, but in stopping fraud ***before*** it happens. Innovation will not stop here. Industry recognizes that consumers want choice, security and convenience.

THE VALUE OF PREPAID CARDS IS TOO BIG TO IGNORE. As Congress and the Administration look for ways to achieve cost savings, simplify the delivery of benefits and payments to individuals, and eliminate fraud, the value of prepaid cards is too big to ignore. The federal government should be consistent in its approach to electronic payments and take lessons learned from states, including the adoption of card-based income tax refund programs.

ISSUE: DELIVERING FEDERAL TAX REFUNDS ON PREPAID CARDS

BACKGROUND: Of the one billion benefit payments totaling $1.7 trillion made by the Treasury in 2010, an estimated $287 billion was disbursed by paper check rather than electronically deposited to a bank account. Although the U.S. Government now requires that all federal *benefit payments* be made electronically, the IRS continues to issue tax refunds either through paper check or electronic deposit. The IRS encourages but does not require tax refunds to be issued electronically and in *tax year 2011, the IRS distributed more than 45 million refund checks.* The IRS is the last remaining federal program not to fully embrace electronic payments.

THE BENEFITS. The switch to the electronic delivery of social security benefits alone is projected to save U.S taxpayers $1 billion over ten years. This is because the cost of disbursing funds by paper checks is substantial: $1.03 per paper check compared to $.10 for an electronic payment. The benefits to recipients and the federal government are also substantial: increased security, transparency, accountability and financial inclusion. For the approximately 80 million households who are unbanked and/or underserved, cashing a check is costly and less secure. Benefit check cashing fees can range from $3.00 to 2%- 6% of the face value of the check. In addition, in one year alone, more than 540,000 Social Security and Supplemental Security Income paper checks were reported lost or stolen and had to be replaced, at a significant cost to the government and inconvenience to the recipient.

THE TAX PILOT. In 2010, IRS conducted a pilot program intended to test multiple scenarios of card-based refunds. With only limited participation, some described it as a "failure". At the same time, the pilot provided valuable lessons learned, including that such a product could be both valuable to tax filers and produce savings to the Department of Treasury. A report by the Urban Institute in January of 2012 concluded that that receiving refunds directly onto a low cost account-linked card was a concept with promise, including access to mainstream financial services for the unbanked. The National Taxpayer Advocate has also repeatedly endorsed the goal of issuing refunds electronically.

THE QUESTION OF FRAUD. According to the Government Accountability Office (GAO), there were 641,690 incidents of identity theft involving tax fraud in 2011. This number is on the rise and remains a top priority for IRS Criminal Investigators. Once a check is issued, there is no pulling it back if fraud is subsequently detected. With electronic payments, funds can be recalled.

THE STATES. Today, 49 of 50 states have implemented card-based electronic payment programs for their constituents across a wide range of government disbursement programs: Child Support, Unemployment Insurance; Temporary Assistance for Needy Families (TANF); Emergency Disaster Relief; Workers' Compensation; Adoption Assistance; Foster Care; and Housing Subsidies for Beneficiaries and Property Owners. Additionally, 10 states are now issuing state tax refunds via electronic means:

- Alabama	- Connecticut
- Georgia	- Illinois
- Louisiana	- Missouri
- New York	- Ohio
- South Carolina	- Virginia

QUESTIONS:

1. The federal government requires that all benefit payments be made via electronic means. This has proven to be very successful: there are immediate cost savings to the government, benefits for the unbanked and underserved, and additional security and safety in the delivery of benefits.

   ✓ *Why hasn't the IRS followed the lead of the rest of the federal government in mandating electronic disbursement of tax refunds?*
   ✓ *What would it take to make this happen? Executive Order? Statutory authorization?*

2. The benefits of electronic payments to agencies, taxpayers, and constituents are widespread and proven across a range of state and federal programs. The 2010 pilot provided valuable lessons learned for a national rollout but IRS has not taken steps to initiate a fully electronic tax refund model.

   ✓ *What plans does IRS have to move forward with a fully electronic refund model for tax refunds?*
   ✓ *What specific lessons learned from the 2010 pilot would be applied to a national rollout?*

3. The IRS continues to aggressively tackle identity theft. Multiple efforts are underway to both prevent and resolve cases of identity theft. There is also significant work being done in the private sector to prevent identity theft. For instance, financial institutions and electronic payment networks are working diligently to ensure their disbursement programs are not used fraudulently.

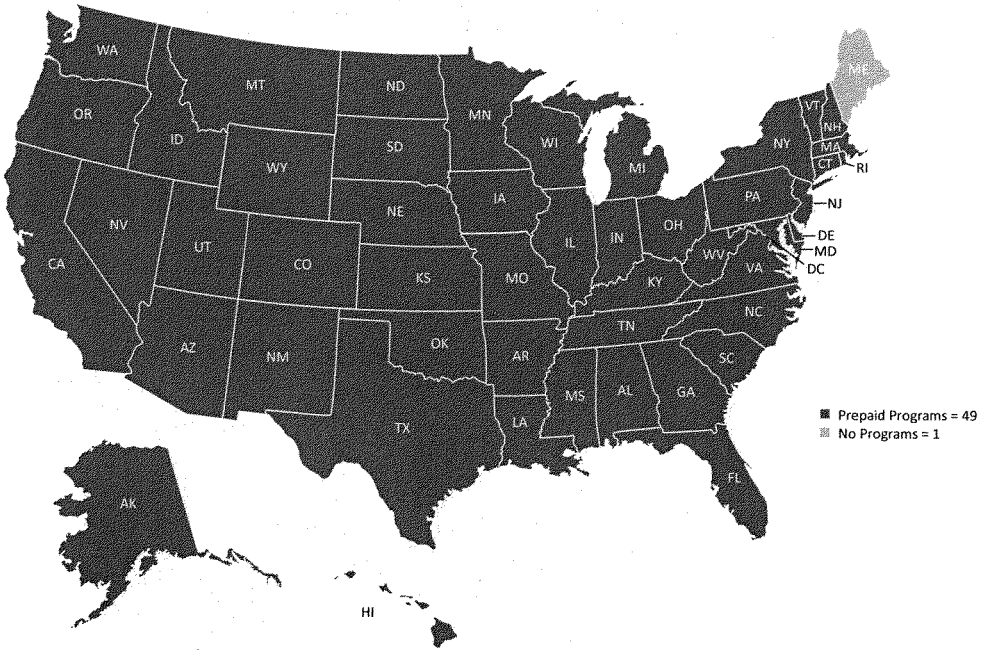
   ✓ *What is the IRS doing to leverage the work being done in the private sector to combat tax fraud in general and identity theft specifically?*

4. A number of states have taken the lead in implementing electronic tax refunds. These efforts will provide additional "lessons learned" at both the state and federal levels. They also potentially offer an opportunity for the IRS to work with these states to issue federal tax refunds.

   ✓ *Can the IRS leverage the work being done at the State level to issue tax refunds electronically?*
   ✓ *Has the IRS been working with these states to determine lessons learned?*

Child Support Prepaid Programs

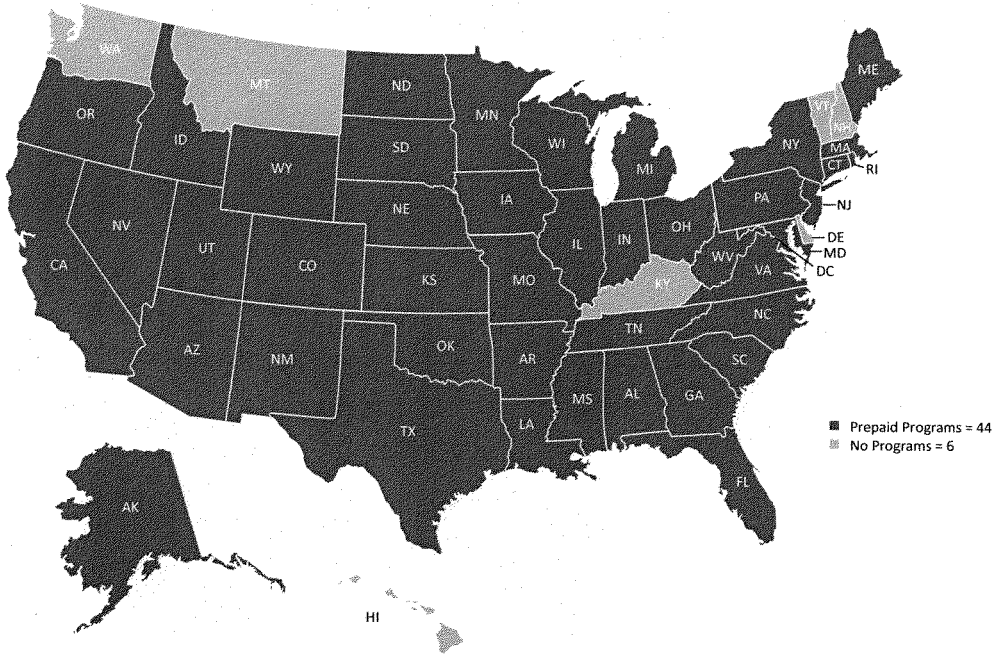
49 States have prepaid Child Support payment programs



Source: Data reflects public information available through individual state agency websites and other publically available information.
The District of Columbia has a Visa-branded prepaid card program for child support payments.
As of 4/2013

Unemployment Insurance Prepaid Programs

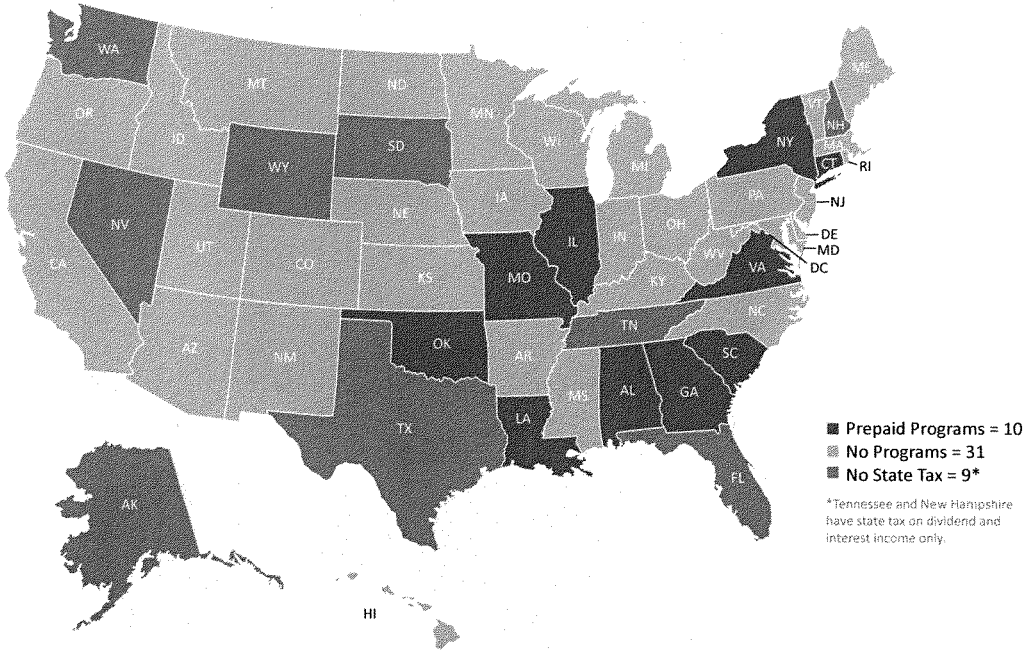
44 States have prepaid Unemployment Insurance disbursement programs



Source: Data reflects public information available through individual state agency websites and other publically available information.
The District of Columbia has a Visa-branded prepaid card program for unemployment insurance payments.
As of 4/2013

State Tax Refund Prepaid Programs

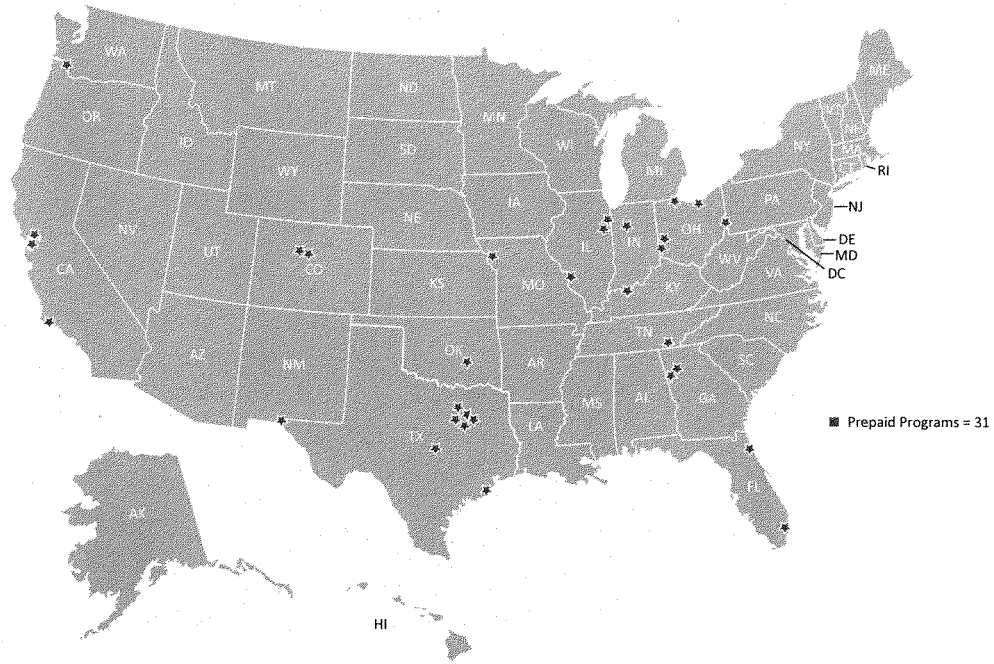
10 states have prepaid Personal Income Tax disbursement programs



Source: Data reflects public information available through individual state agency websites and other publically available information.
As of 4/2013

Housing Authority Prepaid Programs

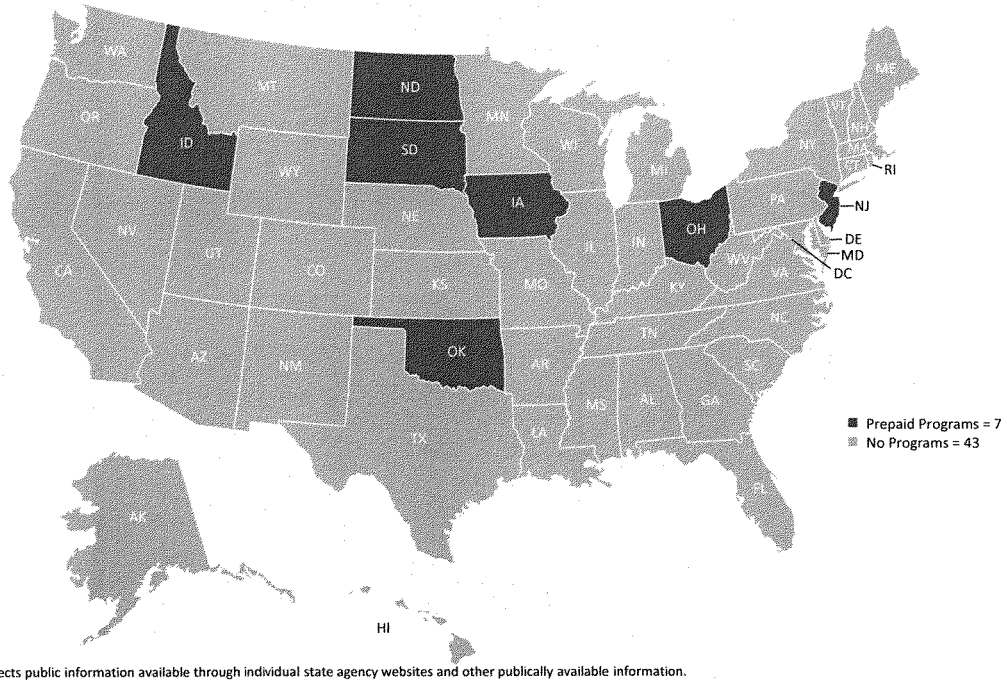
31 counties have Housing Authority assistance disbursement programs



Source: Data reflects public information available through individual state agency websites and other publically available information.
As of 4/2013

TANF Prepaid Programs

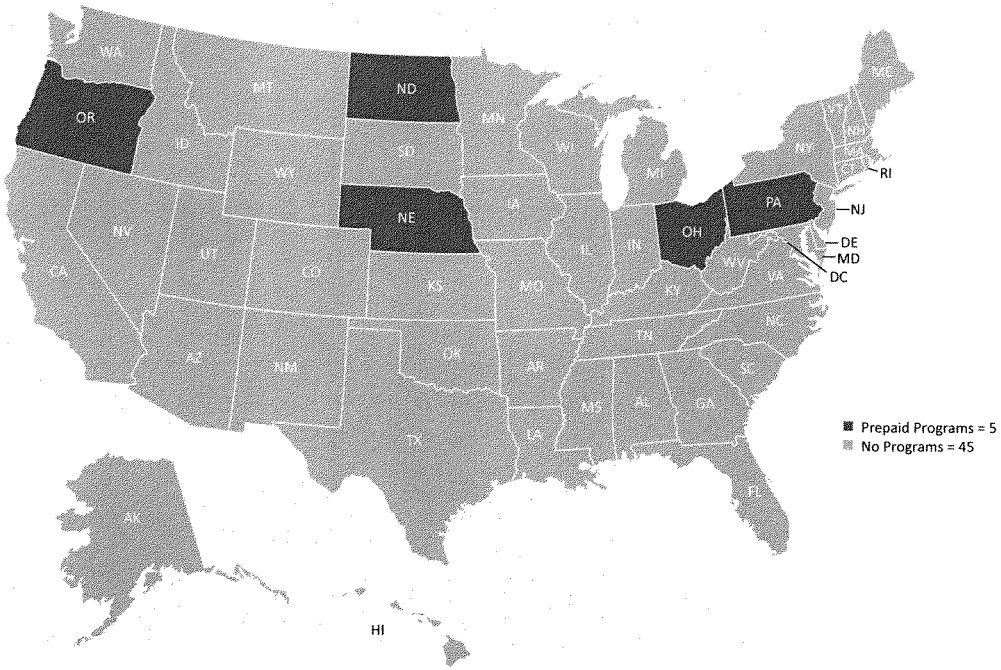
7 states have prepaid TANF disbursement programs



Source: Data reflects public information available through individual state agency websites and other publically available information.
As of 4/2013

Workers Compensation Prepaid Programs

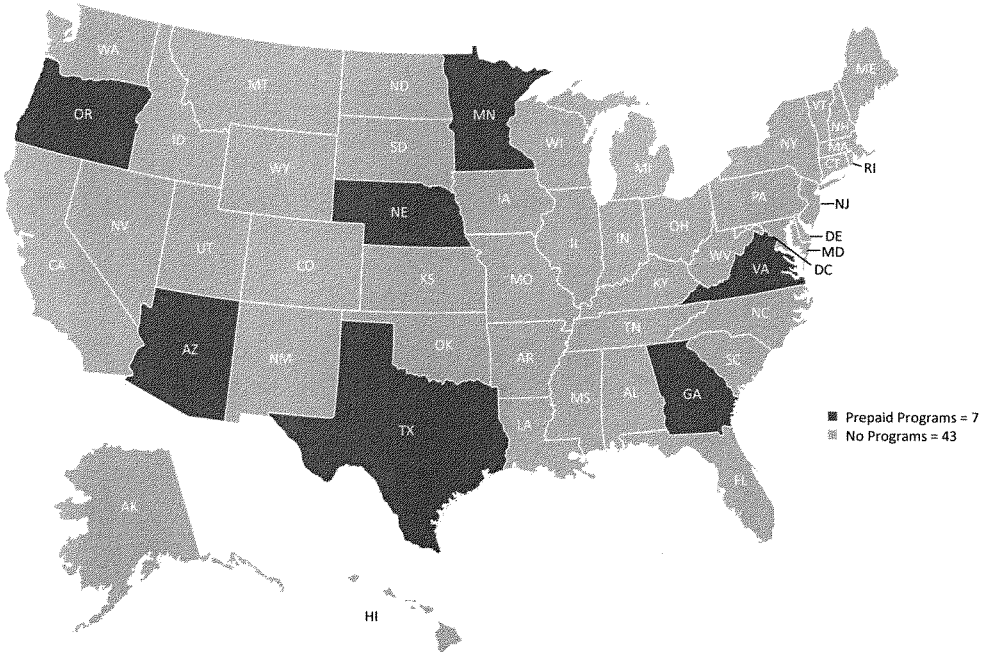
5 states have prepaid Workers Compensation disbursement programs



Source: Data reflects public information available through individual state agency websites and other publically available information.
As of 4/2013

State Payroll Prepaid Programs

7 states have prepaid State Payroll disbursement programs



Source: Data reflects public information available through individual state agency websites and other publically available information.
As of 4/2013