

NATIONAL CONFERENCE OF CPA PRACTITIONERS

22 Jericho Turnpike, Suite 110
Mineola, NY 11501

T: 516-333-8282
F: 516-333-4099

Mr. Chairman and members of the Committee, thank you for inviting me to testify today. My name is Sanford Zinman. I am a Certified Public Accountant, member of the American Institute of CPA's and am currently the National Tax Policy Chair of the National Conference of CPA Practitioners, (**ncCPAP**), as well as the President of the Westchester / Rockland New York Chapter of **ncCPAP**. **ncCPAP** is a professional organization that advocates on issues that affect Certified Public Accountants in public practice and their small business and individual clients located throughout the United States. **ncCPAP** members serve more than 500,000 businesses and individual clients and are in continual communication with regulatory bodies to keep them apprised of the needs of the local CPA practitioner.

I am the sole owner of a CPA firm in White Plains, New York which I started approximately 30 years ago. I have been preparing individual and small business tax returns as well as sales tax and payroll tax returns for over 35 years. I regularly prepare several hundred income tax returns during any given year and am in the trenches with my clients discussing their tax, financial and personal issues and the impact of events on them. Although my clients are mostly in the New York, New Jersey and Connecticut area I have many clients in Florida, Alabama, California, Massachusetts, Nebraska, Tennessee and Washington DC. In this respect my practice is the same as many members of **ncCPAP** and other CPA firms throughout the United States.

According to the Javelin Strategy & Research 2011 Survey Report, the number of US adult victims of identity fraud decreased from 10.1 million in 2003 to 9.3 million in 2005 and 8.4 million in 2007. The total one year fraud amount decreased from \$55.7 billion in 2006 to \$49.3 billion in 2007. There are numerous reasons for these decreases. Much of the change can be attributed to the Identity Theft and Assumption Deterrence Act of 1998. However identity fraud increased by 13% in from 2010 to 2011 when more than 11.6 million adults were victims. Approximately 1.4 million more adults were victimized by identity fraud in 2011, compared to 2010. Much of the increase in identity theft can be attributed to social media and mobile phone behaviors as consumers are still sharing a significant amount of personal information.

The National Taxpayer Advocate's office has also reported growth in identity theft in relation to tax refund fraud. The Identity Protection Specialized Unit (IPSU) which was created by the IRS in 2008 has seen a continuous increase in the number of cases reported to the IRS since the inception of the unit. In Fiscal Year 2009, IPSU had a total of 80,637 cases. In Fiscal Year 2010, this increased to 184,839 cases, and in Fiscal Year 2011, 226,356 cases. This is an increase of over 280% in just two years.

My testimony provides data of which, I am certain, you are already aware. However, the real issue is what identity theft does to individuals and what can be done to combat the problem. It is reasonable to presume that every American has either been personally affected by identity theft or has known someone who

has been a victim. This is a good definition of an epidemic. Identity theft can destroy a person's life. It can prevent them from buying a house or a car, getting a credit card or even having a bank account. It can even hamper someone's ability to get a job. The problem of identity theft will not go away. Attached are a few examples of identity theft problems that have been witnessed and can be shared. The issue is, how can we protect our citizens in an efficient, cost effective manner and what is the government's role in the matter.

During the week of January 23, 2012 the Internal Revenue Service and the Justice Department engaged in a massive national sweep to crack down on suspected identity theft perpetrators as part of a stepped-up effort against refund fraud and identity theft. Working with the Justice Department's Tax Division and local U.S. Attorneys' offices, the nationwide effort targeted 105 people in 23 states. The coast-to-coast effort included indictments, arrests and the execution of search warrants involving the potential theft of thousands of identities and taxpayer refunds. In all, 939 criminal charges were included in the 69 indictments and information related to identity theft. In addition, IRS auditors and investigators conducted extensive compliance visits to money service businesses in nine locations across the country. Approximately 150 site visits occurred to help ensure these check-cashing facilities were not facilitating refund fraud and identity theft. This national effort was part of a comprehensive identity theft strategy the IRS has embarked on that is focused on preventing, detecting and resolving identity theft cases as soon as possible. In addition to the law-enforcement crackdown, the IRS has stepped up its internal reviews to spot false tax returns before tax refunds are issued as well as working to help victims of the identity theft refund schemes. To help taxpayers, the IRS created a new, special

section on the IRS website (www.IRS.gov) dedicated to identity theft matters, including YouTube videos, tips for taxpayers and a special guide to assistance. The information includes how to contact the IRS Identity Protection Specialized Unit and tips to protect against “phishing” schemes that can lead to identity theft. The IRS recommended that a taxpayer who believes they are at risk of identity theft due to lost or stolen personal information should contact the IRS immediately so the agency can take action to secure their tax account. The taxpayer should contact the IRS Identity Protection Specialized Unit. The taxpayer will then be asked to complete the IRS Identity Theft Affidavit, and “follow the instructions on the back of the form based on their situation”.

The Internal Revenue Service has, for many years, recognized the serious issue of identity theft and has instituted measures to combat identity theft and continues to do so. However, many of the IRS “fixes” can be cumbersome and time consuming. Beginning in 2008 the IRS implemented Service-wide identity theft indicators which are placed on a taxpayer’s account if the taxpayer claimed they were a victim of identity theft. But these indicators are implemented only after the taxpayer contacts the Service with certain required substantiation documentation. The IRS can then issue an “Identity Protection PIN” which allows the legitimate taxpayer’s return to bypass the identity theft filters. In mid-November 2011 selected taxpayers received an IP PIN Notice letter notifying them that they would be receiving an IP PIN for use when filing their 2011 return. In mid-December 2011 these taxpayers received a second letter with their IP PIN which was a single-use 6 digit PIN. Some of these letters caused confusion when returns were filed partly because the program was so new. Some letters were

lost which caused problems with filing returns. Some taxpayers forgot to tell their preparers that they received a letter with an IP PIN. Since this was a limited program the negative impact was very limited. Obviously, better communication could result in better outcomes.

In its final report issued on May 3, 2012 The Treasury Inspector General for Tax Administration (TIGTA) indicated that The Federal Trade Commission reported that identity theft was the number one complaint in calendar year 2011, and government documents/benefits fraud was the most common form of reported identity theft. As of December 31, 2011, the IRS's Incident Tracking Statistics Report showed that 641,052 taxpayers were affected by identity theft in calendar year 2011 versus 270,518 in 2010 – a 137% increase. The TIGTA report concluded that the IRS is not effectively providing assistance to victims of identity theft, and current processes are not adequate to communicate identity theft procedures to taxpayers, resulting in increased burden for victims of identity theft. TIGTA found that Identity theft cases are not worked in a timely manner and some cases can take more than a year to resolve. Sometimes communications between the IRS and identity theft victims is limited and confusing, and some victims are asked multiple times to substantiate their identity.

TIGTA recommended that the IRS: 1) establish accountability for the Identity Theft Program; 2) implement a process to ensure that IRS notices and correspondence are not sent to the address listed on the identity thief's tax return; 3) conduct an analysis of the letters sent to taxpayers regarding identity theft; 4) ensure taxpayers are notified when the IRS has received their identifying

documents; 5) create a specialized unit in the Accounts Management function to exclusively work identity theft cases; 6) ensure all quality review systems used by IRS functions and offices working identity theft cases are revised to select a representative sample of identity theft cases; 7) revise procedures for the Correspondence Imaging System screening process; and 8) ensure programming is adjusted so that identity theft issues can be tracked and analyzed for trends and patterns.

The Government Accountability Office (GAO) indicated, in a report issued on June 8, 2012 that the quality of customer service at the IRS has declined noticeably because of budget cuts over the past year and may get worse as the agency is tasked with additional implementation work related to the health care overhaul. The IRS was hit with a 2.5 percent budget cut in fiscal year 2012, with cuts mainly to Enforcement and Operations Support. The cuts took the form of the elimination of 3.1 percent of its full-time employees through attrition, a hiring freeze, and targeted buyouts of more than 900 workers. GAO said data from the Congressional Budget Office justification for the IRS's budget fiscal year 2013 budget request shows that the percentage of phone calls that reach IRS customer service representatives is expected to have fallen to 61 percent in fiscal year 2012, down from 70.1 percent in fiscal year 2011.

It is important that the Treasury and Justice Departments work hand-in-hand to deter identity theft, and impose the severest penalty possible on those who commit it.

As identity theft increases, this also places an additional burden on the tax return preparers. Preparers often find out about identity theft issues after they are authorized to submit a tax return electronically. This only happens after the tax return is prepared, printed and mailed to the taxpayer, and the taxpayer has authorized the electronic submission of the return. On some occasions the delay between the original e-file submission and when the return finally gets filed can affect the taxpayer. States must also be made aware of identity theft problems. In New York a taxpayer's name, address, social security number and birth date are indicated on the tax return. Client copies of returns are mailed to clients for approval. A thief, armed with this information could do irreparable harm.

ncCPAP has been a strong supporter of identity protection for any years. We spearheaded the PTIN regulations for tax preparers to safeguard the preparer's social security number and have partnered with the IRS in the registration of all tax preparers to reduce the number of unscrupulous preparers who try to take advantage of the IRS modernized e-file system. **ncCPAP** has recommended that full social security numbers be redacted from documents (such as Form 1099R, 1099 DIV and 1099 INT) which are mailed to taxpayers. We also recommend that social security numbers be removed from client copies of tax returns that are e-filed. Additionally **ncCPAP** recommends a dedicated IRS Form 14039 (Identity Theft Affidavit) fax line for victims of identity theft. This would speed up the notification process and would also provide an additional level of security compared with the present system of mailing documentation to the IRS. **ncCPAP** also strongly supports H.R. 4362, the STOP Identity Theft Act of 2012 which uses Department of Justice resources with regard to tax return identity theft. We

agree with the concept that no one agency or department can mitigate the problem alone. The problem is too pervasive. We support the concept of the Justice Department working with the Treasury Department. We also support the concept that the federal government reach out to the state governments to attack the problem of identity theft.

Addendum:

Example 1:

I prepare approximately 300 individual returns per year. In the last two years I have had three clients experience Identity theft issues, one in 2010 and two in 2011. Two of the cases involved surviving spouses.

The 2010 incident involved a doctor client who was rejected when we tried to electronically file his return. We filed it before April 15 on paper per the instructions. The client called me the end of May asking where his refund was. About a week later the taxpayer called me back and informed me that he had received written communications from the IRS at his summer residence on Cape Cod (an address never given to the IRS). We finally resolved the issue and secured the client's refund with the help of IRS Taxpayer's Assistance office.

There were two instances of identity theft this past tax season; one was a similar situation with a surviving spouse being rejected when we tried to e-file his return. The other situation involved a taxpayer who received a letter from the IRS stating the refund would be held up for standard identity check. The client's return is on extension and has not been filed yet. In both cases we have filed the proper documentation but no resolution has been reached.

Example 2:

Two separate incidents. The first; I received an e-file rejection for a taxpayer due to a possible identity theft issue. Taxpayer called the IRS numerous times and (according to the taxpayer) got different answers each time. We finally had to submit on paper. The second; I received an e-file rejection indicating that the taxpayer was deceased. I called the taxpayer who told me he received some

notification from the IRS but thought he lost it. He found the IP PIN and we were able to file the return.

Example 3:

Client is a single mom with two elementary school children. One child's social security number was compromised. Neither the parent nor I were aware of this. The IRS never sent the taxpayer a notification. After the e-file was rejected we filed on paper and the refund (in excess of \$4,000.00) took nine weeks to be received.

Example 4:

A taxpayer sent me her tax information in early April. We prepared the return and sent the documents to the taxpayer. We received the authorizations to e-file and did so only to have the return rejected. Neither the taxpayer nor I were able to determine from the IRS the origin of the problem for several days. We paper filed the return and then found out that someone else had e-filed using the taxpayer's social security number.