American Institute of CPAs
1455 Pennsylvania Avenue, NW
Washington, DC 20004-1081

June 27, 2013

The Honorable Max Baucus
Chairman
Senate Committee on Finance
219 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Orrin G. Hatch
Ranking Member
Senate Committee on Finance
219 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Bill Nelson
United States Senate
716 Hart Senate Office Building
Washington, DC 20510

RE: Comments on the Identity Theft and Tax Fraud Prevention Act of 2013 and Recommendations on Efforts to Combat Identity Theft

Dear Chairman Baucus, Ranking Member Hatch and Senator Nelson,

The American Institute of Certified Public Accountants (AICPA) respectfully submits comments on the Identity Theft and Tax Fraud Prevention Act of 2013 as well as our recommendations on efforts to combat identity theft. This letter was developed by the Identity Theft Task Force of the AICPA IRS Practice and Procedures Committee, and approved by the Tax Executive Committee.

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.

## Background

One of the most important topics for our members 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 on 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, as discussed later in our comments, some actions that tax professionals believe would reduce the threat of identity theft would require legislative or regulatory changes.

**Comments on the Identity Theft and Tax Fraud Prevention Act of 2013**

The AICPA has reviewed S. 676, Identity Theft and Tax Fraud Prevention Act of 2013, as introduced by Senator Bill Nelson (hereinafter "Bill"), and we are pleased to provide our initial thoughts on various provisions in the Bill. As we continue to review the Bill in detail, we may provide additional written feedback.

**Bill Provisions Supported by the AICPA**

The AICPA applauds and supports the majority of the provisions in the Bill. We have reserved our initial written comments on the Bill to several provisions we feel are of high importance.

Title I, Section 102. Single Point of Contact for Identity Theft Victims

The AICPA supports the provision that there should be a single point of contact at the IRS for identity theft victims who have had their tax returns delayed or otherwise adversely affected. A single point of contact throughout the processing of their case would provide an identity theft victim a much needed level of comfort and reduce the level of stress and confusion through an extremely difficult time.

Additionally, having one point of contact will streamline IRS efforts in terms of personnel assigned to each case and documentation of each case. Duplication of efforts will be minimized and the "learning curve" caused by having multiple people working on one case without a person to spearhead the efforts and communicate directly with the taxpayer would be eliminated.

Title I, Section 103. Enhancements to IRS PIN Program

The AICPA agrees with section 103 of the Bill which states that a personal identification number (PIN) should be issued as soon as practicable to identity theft victims upon establishing their identity with the IRS. Ensuring that a personal identification number is provided will aid victims in avoiding repeat instances of tax identity theft.

We believe that the IRS has made great progress in issuing PINs but support the issuance of PINs in more instances. The AICPA is recommending an administrative proposal that would provide PINs to additional taxpayers. Our recommendation is discussed later in this letter.

Title II, Section 202. Limitation on Multiple Tax Refunds to the Same Account

The AICPA supports the provision to restrict the delivery or deposit of multiple tax refunds from the same tax year to the same individual account or mailing address. We believe this provision will greatly support the efforts in the reduction of identity theft. We suggest that consideration be given to ensure this effort does not hinder multiple family members living in the same household from receiving appropriate tax refunds.

Title III, Section 301. Restriction on Access to the Death Master File

We support action to restrict and delay access to the Death Master File (DMF), which is a list of deceased persons maintained by the Social Security Administration. Restricting immediate access of the DMF to users with legitimate fraud prevention needs and delaying access to other users is a reasonable way to support fraud prevention efforts.

The DMF contains sensitive information including the full name, date of birth and social security number of decedents. This information is publicly available, making it a prime source of information for identity thieves. This proposal would restrict immediate access to the DMF to groups that have a bona fide need for the information. Access to the DMF by the general public would be delayed.

**AICPA Concerns with Selected Bill Provisions**

While we are in agreement with the majority of the provisions in the Bill, the AICPA believes the following provisions, as currently stated, would not be beneficial to reducing or eliminating identity theft or serve as a deterrent to identity theft perpetrators.

General Comment – Time frames

We understand the urgency in working to resolve the issue of identity theft as expeditiously as possible. However, we feel that many of the regulatory time frames contained in the Bill are unrealistically short.

For example, as stated above, the AICPA supports the concept of improving the handling of identity theft cases by the IRS. We do not, however, support the 180-day time frame stated in Title I and II of the Bill in which to set up the necessary procedures. We think six months is simply not enough time to develop well-reasoned rules and regulations. Too often our members have dealt with unintended negative consequences stemming from hastily drawn regulations. We suggest that providing the adequate time to draft regulations and procedures, and providing additional time for comment from the many-affected stakeholders would be a more workable approach.

We are aware that the IRS is actively studying ways to effectively combat the rising tide of identity theft. We believe that placing an artificial timeline on the issuance of guidance will not lead to better answers and plans going forward. Instead, it will lead to stop-gap measures that do not fully resolve the many problems in the tax system caused by identity theft.

Title IV, Section 402. Increased Penalty for Improper Disclosure or Use of Information by Preparers of Returns

The AICPA strongly objects to the increase in tax return preparer penalties under Internal Revenue Code (Code) sections 7216[1] and 6713 as provided for in the Bill. The focus of efforts to curb identity theft should fall squarely on the causes of identity theft. The true cause of identity theft does not stem from inappropriate behavior by tax return preparers. Thus, increasing the penalties for improper disclosure or use of tax return information by tax return preparers will not deter identity theft.

We believe the existing penalties in sections 7216 and 6713 provide adequate safeguards in the deterrence of identity theft by way of inappropriate actions by tax return preparers and therefore recommend that the penalties remain as currently stated in the Code.

Effective in 2009, Treas. Reg. § 301.7216 addresses modern return preparation practices, including electronic filing and the cross marketing of financial and commercial products and services by tax return preparers.

Absent a specific exception, Treas. Reg. § 301.7216 generally prohibits the disclosure or use of tax return information without the client's explicit, written consent. In general, a "disclosure" of tax return information involves a disclosure by the preparer of a client's return information to a third party. A "use" of tax return information generally involves the use of the return information by the preparer potentially for the purposes of offering non-tax services to the taxpayer.

Under section 7216, a tax return preparer is subject to a criminal penalty for "knowingly or recklessly" disclosing or using tax return information. Each violation of section 7216 could result in a fine of up to $1,000 or one year of imprisonment, or both. Section 6713, the companion civil penalty, imposes a $250 penalty on a preparer for each prohibited disclosure or use of the return information, not to exceed $10,000.

[1] All section references in this letter are to the Internal Revenue Code of 1986, as amended, or the Treasury regulations promulgated thereunder.

This section of the Bill increases the civil section 6713(a) penalty of $250 to $1,000 and increases the overall penalty limit from $10,000 to $50,000. Additionally, the Bill increases the criminal penalty in section 7216(a) from $1,000 to $100,000.

The AICPA believes that increasing penalties in this area will not deter identity theft for two reasons: 1) most tax-related identity theft is not perpetrated by those engaged in the business of tax return preparation; 2) to the extent that tax-related identity theft is perpetrated by persons purporting to be tax return preparers, those perpetrators are subject to more narrowly tailored and more severe penalties in other parts of the IRC and other criminal laws as discussed below. Because there is little deterrent benefit to increasing these penalties, but the potential for unintended and negative consequences for application of such penalties to tax practitioners, we object to this provision of the Bill.

Tax-related identity theft is typically committed with the personal information of individuals who have no filing requirement.[2] For example, senior citizens are prime targets of tax-related identity theft because many have no filing requirement. In these cases, fraudulently filed returns may go undetected because no duplicate return is ever filed using the same Social Security Number.

Also, the personal information used by identity thieves, generally is not obtained as a result of a tax return preparer's disclosure. Rather, it is stolen or found on the Internet (for example, the Social Security Death Master File is recognized as a source of personal information used in identity crimes). The IRS does not appear to keep statistics on the percentage of tax-related identity crimes committed by tax return preparers, but a review of publicized convictions stemming from these crimes suggests that most perpetrators are not engaged in the business of tax return preparation.[3] As sections 7216 and 6713 only apply to those engaged in the business of tax return preparation, those sections would not apply to the majority of tax-related identity theft crimes.

For the tax-related identity theft crimes that are committed by tax return preparers, there are numerous other severe criminal penalties that can be imposed on those individuals who perpetrate those crimes. For example, the crime of identity fraud carries a maximum sentence of 15 years in prison and a maximum fine of $250,000 for each count. The crime of preparation and presentation of false and fraudulent federal income tax returns carries a maximum sentence of three years in prison and a maximum fine of $250,000. Additionally, the Criminal Investigation Unit of the IRS is expanding the number of

[2] November 29, 2012 Testimony of Russell George, Treasury Inspector General for Tax Administration, before the House Committee on Oversight and Government Reform Subcommittee on Government Organization, Efficiency and Financial Management.
[3] See, for example, "Examples of Identity Theft Schemes – FY 2013" at http://www.irs.gov/uac/Examples-of-Identity-Theft-Schemes-Fiscal-Year-2013. The listed 70 cases involved actors involved in fraudulent conduct, not practitioners engaged in legitimate tax return preparation activities.

charges that special agents investigate when identity theft matters arise in order to increase the severity of potential sentences and fines perpetrators may face.[4]

The Bill also seeks to add a new criminal penalty for using a false identity in connection with tax fraud that will impose a maximum sentence of 5 years in prison and a maximum fine of $250,000. The AICPA supports this proposal.

Given the other criminal provisions available to deter tax-related identity theft, increasing the penalties under sections 7216 and 6713 is unnecessary and may have unintended negative consequences if such extreme penalties are applied against members of the tax return preparer community in situations involving inadvertent disclosures or uses of tax return information.

## AICPA Proposals to Curb Identity Theft

In addition to our comments on the Identity Theft and Tax Fraud Prevention Act of 2013, the AICPA would like to present the following recommendations, aimed at combatting identity theft, for your consideration.

### I. Address Change Verification

Background

The IRS recommends that taxpayers properly notify the IRS when they have changed their address to ensure that the IRS sends tax refunds and other correspondence to the correct address. With the growth of identity theft, we recognize the potential problems caused for the IRS in ensuring that taxpayers are provided timely and accurate correspondence regarding their tax accounts. Whether an identity thief chooses to use the address of the "real taxpayer" or change it, problems may be created for the identity theft victim.

The IRS allows change of address notifications to be made by simply writing the new address on a tax return, providing some type of written notification or submitting Form 8822, *Change of Address*. IRS recommends that taxpayers also notify the United States Post Office (USPS) of any change of address so that, if mail is returned to the IRS, taxpayer records can be updated using the address of record which was provided to the USPS that it maintains in its National Change of Address (NCOA) database. A reference in the NCOA website notes that every year over forty million Americans change their place of residence, so it is clear that keeping up with taxpayers can be a challenge. We

[4] April 16, 2013 Testimony of Steven T. Miller, Acting Commissioner of the Internal Revenue Service, before the Senate Finance Committee.

appreciate the problems the IRS encounters in meeting various legal requirements to deliver taxpayer correspondence to the last known address of the taxpayer even without considering potential identity theft issues where the taxpayer may not reside at the address on a return.

We also recognize that there are several federal agencies that rely on addresses in their databases to deliver payments or correspondence on a regular basis to the last known address of their beneficiaries or constituents. It seems these databases might also be used to validate addresses on tax returns when they indicate address changes from year to year. The use of these databases may require the IRS to establish new procedures or policies for receipt of information from other government agencies, but in view of the potential consequences of identity theft, we believe such efforts are warranted.

Recommendation

The AICPA believes that further validation of a taxpayer's address or change of address should be considered as an additional aid in verifying possible fraudulent refund returns, and we offer several recommendations in that regard. When an income tax return is received with an address that is different than the address on the prior year return, before issuing the refund, the IRS could consult the NCOA database to see if the taxpayer has notified the USPS of the same address change. Additionally, by matching limited amounts of data (e.g., name, address and social security number) from other federal data bases to that same data on income tax returns, the IRS may be able to mitigate refund fraud using identity theft. Another suggestion for taxpayer verification involves asking taxpayers who are claiming refunds for additional information on their tax return. For example, a taxpayer could provide the amount of their prior year's adjusted gross income (AGI) when filing their current year tax return. We would suggest making this question optional if the taxpayer wants to "expedite" the processing of his or her refund. If the taxpayer decides not to provide the AGI (or other requested information) then his or her refund would be delayed pending further verification.

It is our understanding from a reading of Internal Revenue Manual (IRM) 5.1.18.12 that when the USPS receives a change of address from a taxpayer, the IRS will receive that new address. The NCOA receives this information and provides a weekly NCOA report of all the changes for the week. If this information is matched to the Master File address, it appears that the taxpayer address is then updated. While realizing there is the potential for identity thieves to use this process in updating an address, we believe it may serve as a chance to perform an additional validity check on tax returns for which address changes do not show up in the NCOA.

We also believe that by comparing Social Security Numbers (SSNs) and addresses on suspected fraudulent refund returns with SSNs and addresses on data bases of other

federal agencies that remit checks or electronic funds to taxpayers or citizens, some instances of identity theft may be identified. This belief is based on an assumption that the addresses on fraudulent refund returns are usually not the address of the identity theft victim. If an address associated with a SSN on an income tax return does not match the address on remittances of money that bear the same SSN of benefit recipients, there is a strong possibility that the refund return may be fraudulent because recipients of remittances from federal government agencies usually are careful to keep those agencies apprised of the current address at which to receive such funds.

Examples of federal agencies where this matching of addresses may be productive include the U.S. Social Security Administration that provides monthly social security and disability checks to individual taxpayers, the Department of Defense that provides payments to military and civilian personnel, and the Veterans Administration that potentially makes remittances to individuals and/or medical providers where SSNs may be associated with those remittances.

We understand that these recommendations add another check to the processing of tax returns that may delay refunds but given that identity theft has become such a huge problem in this country, we believe that the additional validation is justified.

## II. Identity Protection Personal Identification Number

Background

The IRS has established a system to issue an Identity Protection Personal Identification Number (IP PIN) to certain taxpayers whose identity has already been stolen or potentially compromised. Recent IRS information indicates that the IRS issued more than 600,000 IP PINs to victims of identity theft. While this number seems astounding, it has been reported by Government Accountability Office (GAO) and U.S. Treasury Inspector General for Tax Administration that the number of incidents may be significantly higher. Therefore, the AICPA believes that taxpayers should be able to request and obtain an IP PIN before identity theft has occurred.

The consequences of identity theft can be severe, particularly if an individual's personal tax records have been affected. The time required for a taxpayer to correct compromised federal tax records is substantial, with recent estimates stating nine to twelve months or longer to get resolution. Additionally, taxpayers who choose to engage a tax professional to correct federal tax records must generally spend a material amount on professional fees.

The IP PIN system is an existing "on the shelf" means to prevent fictitious tax returns from being filed using an individual's Social Security Number. The IP PIN is obtained by

filing Form 14039, *Identity Theft Affidavit*. Form 14039 must be accompanied by proof of identity, such as a copy of a passport, driver's license or Social Security Card. As such, the expansion of the IP PIN system would not require the IRS to establish new procedures or policies.

Recommendation

The AICPA believes that the IP PIN system should be expanded to include a taxpayer "opt-in" option, which would ultimately save the Service time and money by reducing identity theft-related compromises to federal income tax records. However, we also recognize that the IRS may not be in a position to accommodate a significant increase in the volume of IP PIN requests. As such, we believe that the IRS should consider imposing a one-time "user fee" upon taxpayers who want an IP PIN but have not been identified by the IRS as subject to identity theft. The user fee could be used to fund the increase in personnel necessary to accommodate the increase in requests for IP PINs.

The AICPA also believes that many taxpayers would readily pay a reasonable one-time fee for the additional security afforded by obtaining an IP PIN. We believe that the demand for this security is the recognition by taxpayers of the severe consequences of the identity theft-related compromise of federal tax records and represents a pro-active choice to save time and resources in response to this potential threat. It is important to note that many U.S. citizens already pay private companies for credit monitoring services indicating a demand for such. Indeed, a "credit freeze" is now available in most states.

We understand that the IRS has a daunting task before them and is considering ways to implement more advanced authentication systems and procedures. While we applaud such efforts, we are very concerned that such efforts may not result in additional security for taxpayers until well into the future, or will only impact taxpayers that have been identified by the IRS. As such, we believe that expanding the use of the existing IP PIN process allows for the most rapid increase in security for all taxpayers and a reduction in the occurrence of identity theft and fraudulent tax refunds.

## III. Truncated Taxpayer Identification Numbers

Background

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.[5] 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 SSNs 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.

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.

Recommendation

We understand that limitations exist currently with regards to truncation on a Form W-2, *Wage and Tax Statement*. Under section 6051(a)(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.

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.

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

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.

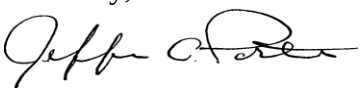
**Conclusion**

While the AICPA is overwhelmingly in support of efforts focused on combatting identity theft, we believe care must be given to target those efforts towards the areas of greatest risk. In that regard, we support enhancements to the PIN program, restricting access to the Death Master File, limiting multiple refunds to the same account, address change verification efforts, as well as enhancements to the IP PIN program. We do not feel that tax return preparers are the cause of identity theft and therefore, do not support increases to the existing penalties for unauthorized disclosures of tax return information.

* * * * *

We appreciate your consideration of our comments and recommendations, and we welcome further discussion. If you have any questions, please contact me at (304) 522-2553, or jporter@portercpa.com; Kathy Petronchak, Chair, IRS Practice and Procedures Committee, at (202) 758-1480, or kpetronchak@deloitte.com; or Kristin Esposito, AICPA Technical Manager, at (202) 434-9241, or kesposito@aicpa.org.

Sincerely,



Jeffrey A. Porter, CPA
Chair, Tax Executive Committee

cc: Mr. Daniel Werfel, Principal Deputy Commissioner, Internal Revenue Service
The Honorable Mark Mazur, Assistant Secretary (Tax Policy)
The Honorable William J. Wilkins, Chief Counsel, Internal Revenue Service