NATIONAL **C**ONFERENCE OF **CPA P**RACTITIONERS

22 Jericho Turnpike, Suite 110 *T: 516-333-8282*

Mineola, NY 11501 F: 516-333-4099

Chairman Chabot, Ranking Member Velazquez and members of the Committee, thank you for inviting me to testify today. My name is Stephen Mankowski. I am a Certified Public Accountant, Executive Vice President of the National Conference of CPA Practitioners, (**NCCPAP – the countries' second largest CPA organization**) and a member of the American Institute of CPAs (AICPA). **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 one million business and individual clients and are in continual communication with regulatory bodies to keep them apprised of the needs of the local CPA practitioner and its clients. Accompanying me is Mr. Sandford Zinman, National Tax Policy Chair of **NCCPAP**.

My firm, E.P. Caine & Associates CPA, LLC, has been preparing tax returns for over 30 years. My firm annually prepares well over 2,000 small business and individual tax returns as well as sales tax returns, payroll tax returns, highway use tax returns and Forms W2 and Forms 1099 informational returns. We are in the trenches with clients discussing their tax, financial and personal issues, and the impact events and proposed tax law changes may have on them. Although our clients are mostly in the Pennsylvania, New York, New Jersey and Delaware areas, we serve clients in over 30 states and also provide services to clients in Canada and

Europe. In this respect our practice is the same as many members of **NCCPAP** and other smaller CPA firms throughout the United States.

NCCPAP has been at the forefront of identity theft issues through our advocacy and testimony at prior hearings dealing with ID theft in June 2012. The initial hearings focused on the refund scams that were prevalent at the time, such as Mo Money. **NCCPAP** has remained vigilant on the topic and has been discussing these issues annually when our members meet with Congress and their staff and with IRS representatives. Our members have helped guide numerous taxpayers who have been victims of ID theft to navigate through the IRS to minimize the risk of further consequences.

ID theft has been growing exponentially for years. It seems that no matter what controls are put in place, criminals have better and more focused resources to circumvent these safeguards. All businesses are at risk, from the largest to the smallest. Weekly, we are hearing about the latest business to be a victim of some level of cybercrime or ID theft. Mr. Richard Snow, who is also on the panel of witnesses today, has been a victim.

All businesses are at risk, but CPA firms and tax practitioners are at a greater risk. The IRS reminds tax preparers that they must be vigilant with their system integrity. The criminals are aware that the "prize" for breaching tax practitioner systems could yield them not only names and social security numbers, but also several years of earnings as well as bank information and dates of birth. Thus, the IRS recommends that tax preparers create a security plan. IRS Publication 4557,

Safeguarding Taxpayer Data, provides suggestions and a checklist. My firm has reviewed the Publication, continually trains our staff and, along with our IT consultants, monitors our information and controls to ensure that our offices not only meet but exceed these suggestions. Our network logs usage from all users and is monitored to ensure no unauthorized access. This includes staff with remote access to our server. We also require a user id and passwords to gain access to all of our software packages. Not all firms have been as fortunate regarding cyber security. Two Midwestern firms were compromised this tax season and had fraudulent returns filed through their electronic filing identification number (EFIN).

I was able to speak with a partner at one of the affected firms. They were under the impression that their systems were secure. However, the breach occurred after installing a new copier system that had not been properly secured within their network. Once they determined that they did in fact have a breach, they attempted to contact the IRS. Unfortunately, there is no easy means to identify the proper area within the IRS to contact. Ultimately, it took nearly one month for a response from the IRS.

Ensuring the security of client data has been and remains the goal of my firm and we take that task very seriously. Although our software has the ability to auto-generate the PINs for electronic filing (EF PIN), we became aware that the EF PIN was using a portion of the taxpayer SSN. We have opted to not use this part of our software and have chosen to manually enter the EF PIN. Some tax software packages use a random five-digit number and we have suggested our software

provider offers the same option. Taxpayers are also able to obtain their own specific EF PIN through the IRS website through the entry of select information. Currently, this system is too new to ascertain the true effectiveness of the program; however, concerns exist as to whether the return would reject if this number was not used or what would happen if the taxpayer lost this number. It is not clear if there is a mechanism to retrieve the number from the IRS.

Practitioners are also reminded to protect their EFIN. The IRS suggests practitioners log into e-services on a regular basis and verify the number of returns processed for their EFIN. While the number probably will not be exact due to the timing of return processing and updating of this service, significant differences could be a cause for alarm. Practitioners should contact the IRS e-Help Desk immediately if the difference is excessive. At the beginning of this filing season, the tax software community requested that tax practitioners update their EFIN authorization letter before they start using their EFIN. This is just another step in preventing potential unauthorized access to a practitioner EFIN. While in many cases the timing of this request might not have occurred at the most opportune time, such as when the first returns were to be filed, it sent a signal to the practitioner community that the software vendors understood the issues and were working in conjunction with practitioners to address ID theft.

While firms that electronically submit tax returns are required to obtain an EFIN from the IRS, paid preparers initially included their social security number on tax returns and in 1999 were first offered the ability to use a Preparer Tax Identification Number (PTIN). The requirement to include the preparer's firm

information, which includes their employer identification number, began in 1978. Given the risks of firm ID theft, why has the IRS not adopted a firm PTIN?

There are two primary reasons that criminals attempt to breach systems– the challenge and/or for the information contained in the systems, both reasons for IRS action. The IRS has been transitioning to modern technology within its network protocols to enhance safeguards. During this transition, the IRS has encountered many of the same compatibility concerns that affect most businesses. As a CPA, I became aware of this when the IRS announced the planned retirement of the Disclosure Authorization (DA) and Electronic Account Resolution (EAR) options on IRS e-services in August 2013. When the tax practitioner community complained that the elimination of these options would have a significant impact on their practices, we were told that the platform on which these services were designed was not compatible with the new system architecture and the initial costs to rewrite the programming was excessive. The IRS has looked at a relaunch of these services in the future, but the added authentications might make the systems overly burdensome.

In March 2015, one tax software vendor had its electronic processing systems compromised to the extent that the state of Minnesota and subsequently all states temporarily ceased accepting electronically filed returns from that vendor. One positive result of this situation was the formation of the IRS Commissioner's Security Summit, which initially included representatives from state governments, banking and the software community. This group approach was a positive signal from the IRS that the issues of identity theft and data security required a multi-

faceted approach to work at stemming the increases in data security and ID theft. Their initial focus was addressing and stopping suspected fraudulent returns through the implementation of protocols to address issues with tax returns before processing and during the initial processing. According to a recent General Accounting Office (GAO) report, it is estimated that during the 2014 filing season the IRS paid approximately $3.1 billion in fraudulent refunds while preventing $22.5 billion. This was before the creation of the Security Summit.

In its initial year, the Summit estimates that it has prevented in excess of three million fraudulent returns from being processed and refunds issued during the 2015 filing season, but many fraudulent returns are still getting through. The Summit has now been expanded to include tax practitioners. The next level of focus needs to be on securing the refund process. According to Senator Wyden, the IT budget within the IRS is now operating at a level lower than it was six years ago due to budget cuts. The criminals, however, have ample cash and sophisticated systems. They continually attempt to reverse engineer the security measures implemented by the IRS. One recent instance occurred when the IRS announced that only three IRS refunds would be able to be direct deposited into a bank account in any calendar year. It was determined that adding zeros before the account number would trick the IRS systems to think it was a different account number and allow the refunds to be deposited. It satisfied the IRS systems while being disregarded by the financial institutions. This was a case that I believe the IRS learned a valuable lesson – while you can publicly address the solutions being implemented, you should not provide the specifics. The limitation of refunds was designed as a deterrent, but ultimately only served as a means of preventing tax preparers from illegally collecting the fees from a taxpayer refund.

The timing of the receipt of data by the IRS often comes into question. Often fraudulent returns are submitted with refunds transmitted long before the data needed to verify the income and the tax withholding is received by the IRS. Businesses filing Forms W-2 on paper are required to submit the data by the end of February, while electronic filers had an additional 30 days. In addition, an automatic 30-day extension had been available. Because of the delay in submission of these information returns, the criminals have begun filing fraudulent W-2s. In an effort to counter this practice, Congress has removed the automatic extension for filing paper or electronic information returns. However, a time discrepancy still remained. The Protecting Americans from Tax Hikes Act of 2015 (PATH) clarified and simplified these dates. For tax years beginning in 2016, Forms W-2s will be required to be submitted to Social Security and Forms 1099-MISC will be required to be submitted to the IRS with the same due date as to the recipient. This accelerated timeframe should pose a significant hindrance for those who submit fraudulent returns. However, there is still the issue that the IRS will start processing tax returns during the month of January, usually on or about January 20, leaving a window for fraudulent tax returns to be submitted and processed before the IRS has the opportunity to match data.

The IRS has estimated that it averages approximately one million breach attempts daily. However large that number might be, as a taxpayer I would expect that every attempt would be defeated. Unfortunately, over the past year, the IRS has had actual system breaches. First, the IRS online transcript program, "Get Transcript", was compromised in May 2015 and the number of accounts that the IRS admitted were affected has doubled several times. In February 2016 the IRS

announced the affected accounts exceeded 700,000. The second breach that occurred recently related to the Identity Protection PIN (IP PIN) retrieval tool that is contained on the IRS website and is more troubling than the prior breach. The taxpayers who have IP PINs have already been victims of tax refund fraud and obtained the six digit IP PIN to prevent further unauthorized access or filings. This tool had been using the same interface as Get Transcript but had remained available to the public and, unfortunately, those less scrupulous. Finally, the IRS took this page offline in February 2016, nearly nine months after the initial Get Transcript breach.

The March 2016 GAO report identified that the IRS has improved access controls, but noted that weaknesses still remain. One of the primary concerns addressed by the GAO surrounds the authentication of the user ID. The IRS has employed a multifactor approach using two or more factors to achieve authentication. This provides the basis for establishing accountability and for controlling access to the system. Their systems require that Homeland Security Presidential Directive 12-Compliant Authentication be implemented for IRS local and network access accounts. This involves password-based authentication with passwords that are not found in dictionaries and expire at a maximum of 90 days. This same protocol should be implemented for all user accounts, including e-services.

The direct deposit of refunds is a fast, inexpensive and relatively secure means of issuing refunds. The IRS utilizes banking's ACH system, whereby a refund goes to a selected financial institution based upon their respective routing or ABA number. If an account number exists within the institution, the refund goes into the

account. The IRS is mandated to process refunds within 21 days, unless additional processing time is required. Prior to the current Modernized e-File (MeF) system, the IRS had been operating on a "accept by Thursday, refund following Friday" schedule. Often under the MeF system, refunds have been processed even quicker. Taxpayers have grown accustomed to getting the quick refund and now wonder if there is a problem when it is taking longer than a week for their refund to appear in their account.

Social Security Administration uses a banking "pre-note" to verify the accuracy of the recipient's banking information prior to the initial payment. The financial institution has five days to verify the information and notify SSA if there are errors or discrepancies. Failure to notify SSA could result in the institution being held liable for the funds if the funds are misdirected. Unfortunately, the IRS refund system does not include pre-note account verification. Funds are simply transmitted through the ACH network to the respective institution. Once deposited, there is no control on the usage of funds and often where there is fraud those deposits are moved immediately upon receipt. The implementation of a pre-note system could result in a significant reduction of the annual $3.1 billion misappropriation of government funds.

As discussed, Congress has mandated 21 days for refunds to be processed. While it is easy to understand that taxpayers want their refunds processed as quickly as possible, one must ask a simple question. Is paying a tax refund in seven to ten days a prudent use of taxpayer dollars? A recent survey by Princeton Research Associates noted that 22% of taxpayers surveyed would wait up to six to eight

weeks for their refund if they knew it would combat identity theft. **NCCPAP** members feel that simply using the pre-note technology that already exists and is used throughout the financial industry would allow taxpayers to receive their refunds promptly while reducing fraud.

Unfortunately, despite all of the efforts of the IRS and Congress to curb ID theft, often the cause is unscrupulous preparers that are often unregulated by any authority. **NCCPAP** urges Congress to pass legislation to provide the IRS the necessary authority to regulate all tax preparers and required paid preparer to meet minimum standards. Currently, only CPAs, EAs and attorneys are subject to the requirements of IRS Circular 230.

In conclusion, ID theft is an issue that initially gained traction with Congress in 2012. Much has occurred since the initial hearings and, unfortunately, the criminals have taken more steps to obtain information than the IRS has been able to block. The IRS is not alone in this battle. It seems that not a week goes by where there is not news of a major corporation announcing that their systems had been hacked. Taxpayers have become victims of ID theft through these breaches and do not necessarily understand the importance of contacting the IRS. While knowing that the IRS successfully thwarts approximately one million breach attempts each day is comforting, we should keep in mind that even one successful breach could be catastrophic to not only the IRS but to the taxpayer. Often, taxpayers do not realize they have been a victim of ID theft until their electronically filed tax return gets rejected. Once a taxpayer has been victimized, they expect to obtain an IP PIN from the IRS and starting in January 2017 they

will. In Florida, Georgia and Washington, DC where ID theft has been rampant, the IRS implemented a voluntary IP PIN program. Unfortunately, this program failed to achieve the number of participants to make the program successful.

Taxpayers are urged to protect their personal data, but with widespread Internet usage, online shopping and criminals waiting to pounce on unsuspecting victims, ID theft continues to grow. Individual and businesses remain targets of cyberattacks and must remain cautious when opening emails and attachments, visiting web pages and simply paying for the family groceries.

There are several electronic filing options available to taxpayers. Many taxpayers use Free File, thirteen IRS-approved free e-filing tax service sites. In a recent audit performed by the Online Trust Alliance (OTA), six of the thirteen websites failed due to poor site security and not taking steps to help protect consumers from fraudulent and malicious email.

IRS Commissioner Koskinen had the foresight to convene the initial Security Summit in 2015, which has proven to be successful. Unfortunately, the criminals always seem to be pushing the envelope further and further. Their approach is more focused and better funded. The Security Summit has now expanded its focus to include additional user groups, including tax practitioners, to further address cyber security and develop a multi-tiered approach to combat it. The only way to truly combat ID theft is to incorporate input from various sectors of the marketplace. This is a problem impacting businesses and taxpayers worldwide and will require global efforts to minimize and hopefully resolve. **NCCPAP** calls on

Congress to provide the necessary funding to continually monitor, modernize and upgrade IRS systems to minimize and eliminate data security breaches. The first step would be Congress reauthorizing Streamlined Critical Pay Authority to allow the IRS secure top IT talent without a three to six month waiting period.

Thank you for the opportunity to present this testimony and I welcome your questions.

Respectfully submitted,

Stephen F. Mankowski, CPA
Executive Vice President, **NCCPAP**