WRITTEN TESTIMONY OF
JOHN A. KOSKINEN
COMMISSIONER
INTERNAL REVENUE SERVICE
BEFORE THE
SENATE BUDGET COMMITTEE
ON IDENTITY THEFT AND REFUND FRAUD
AUGUST 26, 2015

Senator Ayotte and members of the Committee, thank you for the opportunity to discuss the IRS' efforts to combat stolen identity refund fraud and protect taxpayer information from cybersecurity threats.

Securing our systems and protecting taxpayers' information is a top priority for the IRS. Even with our constrained resources, which are a result of cuts to our budget totaling $1.2 billion since fiscal year 2010, we continue to devote significant time and attention to this challenge. Last fiscal year the IRS committed over $430 million – a 20-fold increase over a span of five years – to fight refund fraud. It is clear, however, that criminals have been able to gather significant amounts of personal information as the result of data breaches at sources outside the IRS, which makes protecting taxpayers increasingly challenging and difficult.

The problem of personal data being used to file fraudulent tax returns and illegally obtain refunds exploded from 2010 to 2012, and for a time overwhelmed law enforcement and the IRS. Since then, we have been making steady progress within our reduced resources, both in terms of protecting against fraudulent refund claims and criminally prosecuting those who engage in this crime. However, we can do much more to protect taxpayers and prosecute criminals with the resources requested in the President's Budget.

Over the past few years, approximately 2,000 individuals have been convicted on federal charges related to refund fraud involving identity theft. More than 400 special agents from the IRS' Criminal Investigation (CI) division continue to conduct tax-related identity theft investigations, with the number of active cases now totaling approximately 1,700. Since 2013, the IRS has initiated more than three dozen cases that involve one or more victims who are New Hampshire residents. The average prison sentence for identity theft-related tax refund fraud grew to 43 months in Fiscal Year (FY) 2014 from 38 months in FY 2013, with the longest sentence being 27 years. We have committed these CI resources despite a 15 percent reduction in the number of special agents from FY 2010 to July 2015.

State and local law enforcement agencies in New Hampshire and around the country also play a critical role in fighting identity theft and bringing identity thieves to justice, and they are pursuing additional investigations and convictions beyond those included above. CI works in close collaboration with its federal law enforcement partners as well as state and local law enforcement to investigate crimes involving tax-related identity theft.

During Calendar Year (CY) 2014, the IRS again protected more than $15 billion in refunds, including those related to identity theft. We continue to improve our efforts at stopping fraudulent refunds from going out the door. For example, we have improved our processing filters, allowing us this year to suspend about 3.2 million suspicious returns and hold them for further review, an increase of over 500,000 from the year before.

Importantly, the IRS continues to work to help taxpayers who have been victims of identity theft. The IRS has 3,000 people working directly on identity theft-related cases, and we have trained more than 35,000 employees who regularly work with taxpayers, so that these employees have the tools to help with identity theft situations should they arise.

We recently completed our efforts to centralize victim assistance with our new Identity Theft Victim Assistance organization. With this new organization, we have consolidated work being done by four different parts of the IRS into one business operating division. This consolidation will improve consistency, program oversight and strategic direction. It is also important to note that we provide taxpayers victimized by identity theft with a single point of contact at the IRS via a special toll-free telephone line.

Taxpayers who become identity theft victims in 2015 can expect to have their situations resolved in less than 120 days, far more quickly than in previous years, when cases could take over 300 days to resolve. While this marks a significant improvement, we are continuing to work to find ways to shorten this time and ease the burden identity theft places on its victims. In CY 2014, the IRS worked with victims to resolve and close approximately 826,000 cases.

Another way the IRS has been assisting taxpayers is through the issuance of Identity Protection Personal Identification Numbers (IP PIN), which protects returns at the time they are filed. For the 2015 filing season, the IRS issued IP PINs to 1.5 million taxpayers previously identified by the IRS as victims of identity theft. Also during this period, the IRS notified another 1.7 million taxpayers that they were eligible to visit IRS.gov and opt in to the IP PIN program. Additionally, taxpayers living in Florida, Georgia and Washington, D.C. – three areas where there have been particularly high concentrations of stolen identity refund fraud – are eligible to participate in a pilot where they can receive an IP PIN upon request, regardless of whether the IRS has identified them as a victim of identity theft.

Another aspect of our work against stolen identity refund fraud involves communicating with taxpayers about the threat posed by identity theft generally, and explaining the steps they can take to protect their personal information and decrease their chances of becoming victimized – everything from changing passwords periodically to checking their credit report annually and using anti-spam software on their personal computers.

But even though the IRS has improved its ability to stop individuals from perpetrating stolen identity refund fraud, we continue to see an increase in organized crime syndicates engaging in these crimes. The IRS is working closely with law enforcement agencies in the U.S. and around the world to prosecute these criminals and protect taxpayers.

The fact remains, however, that these cyber criminals are using increasingly sophisticated means to steal personal information from a variety of sources, and gain access to even more sensitive data than in the past. A good illustration of this problem is the unauthorized attempts to gain access to our Get Transcript application earlier this year. In regard to these attempts, the criminals had already accumulated significant amounts of stolen taxpayer information from other sources, which allowed them, in some cases, to access individuals' prior-year tax returns. We shut down the Get Transcript application, and it will remain disabled until we make modifications and further strengthen security for this application, including by enhancing taxpayer-identity authentication protocols.

To improve our efforts against this complex and evolving threat, the IRS held a sit-down meeting in March with the leaders of the electronic tax industry, the software industry and the states. We agreed to build on our cooperative efforts of the past and find new ways to leverage our public-private partnership to help battle stolen identity refund fraud. Motivating us was the understanding that no single organization can fight this type of fraud alone.

We spent 12 weeks studying what needed to be done, and in June we announced an initial set of new steps to provide stronger protections for taxpayers and the nation's tax system. The steps we agreed to take together represent a new era of cooperation and collaboration between the IRS, the states and our industry partners. For example, IRS partners agreed to expand sharing of fraud leads and to develop stronger methods of authenticating taxpayers when they file their returns. They also agreed to do more to inform taxpayers and raise awareness about the protection of sensitive personal, tax and financial information. Additionally, tax industry members agreed to align with the IRS and states under the National Institute of Standards and Technology (NIST) cybersecurity framework to promote the protection of information technology infrastructure.

The critical point for taxpayers and practitioners to understand is that new protections will be in place by the time they have to file tax returns in 2016. We and our partners will all be making substantive changes through the summer and fall to be ready for the next tax season, and our combined efforts here will better prepare all of us for 2016 and beyond.

This means that the federal government, states and private industry will stop more fraud related to identity theft up front. We will catch more fraud in the IRS security filters during tax processing. And to the extent fraudulent returns do get through, we will have better post-filing analytics to determine ways to adjust our security filters. We will also improve our methods of tracking down the criminals, and add to those approximately 2,000 individuals already serving jail time for federal tax-related identity theft.

Our efforts will also include ensuring that authentication protocols become more sophisticated, moving beyond information that used to be known only to individuals but now, in many cases, is readily available to criminal organizations from various sources. We must balance the strongest possible authentication processes with the ability of taxpayers to legitimately access their data and use IRS services online. The challenge will always be to keep up with, if not get ahead of, criminal syndicates that continue to devote significant amounts of time and resources to victimizing taxpayers.

It should be noted that the collaborative efforts I have described will not end with the actions underway to prepare for the upcoming filing season. The IRS and its partners will continue to work together to address longer-term issues facing the tax community and taxpayers in the efforts against stolen identity refund fraud. We want to ensure that we make lasting changes. These changes are being built into the DNA of the entire tax system.

Congress plays an important role in the fight against stolen identity refund fraud. Congressional approval of the President's FY 2016 Budget request for the IRS is critical. The request includes $140 million in base cybersecurity funding with an additional $101 million for two new initiatives specifically devoted to cybersecurity, identity theft, and refund fraud. An additional $180 million for cyber and identity theft-related critical information technology infrastructure, enhanced enforcement, and secure service options is also included. It is important to note that while the IRS' enacted information technology budget has decreased by 9 percent since FY 2010, private sector investment in cybersecurity is increasing rapidly.

Another way Congress can help in this fight is by passing several important legislative proposals in the President's FY 2016 Budget proposal, including the following:

- ***Acceleration of information return filing due dates***. Under current law, most information returns, including Forms 1099 and 1098, must be filed with the IRS by February 28 of the year following the year for which the information is being reported, while Form W-2 must be filed with the Social Security Administration (SSA) by the last day of February. The due date for filing information returns with the IRS or SSA is generally extended until March 31 if the returns are filed electronically. The Budget proposal would require these information returns to be filed earlier, which would assist the IRS in identifying fraudulent returns and reduce refund fraud, including refund fraud related to identity theft.

- ***Correctible error authority***. The IRS has authority in limited circumstances to identify certain computation or other irregularities on returns and automatically adjust the return for a taxpayer, colloquially known as "math error authority." At various times, Congress has expanded this limited authority on a case-by-case basis to cover specific, newly enacted tax code amendments. The IRS would be able to significantly improve tax administration – including reducing improper payments and cutting down on the need for costly audits – if Congress were to enact the Administration's proposal to replace the existing specific grants of this authority with more general authority covering computation errors and incorrect use of IRS tables. Congress could also help in this regard by creating a new category of "correctible errors," allowing the IRS to fix errors in several specific situations, such as when a taxpayer's information does not match the data in certain government databases.

- ***Authority to require minimum standards for return preparers***. In the wake of court decisions striking down the IRS' authority to regulate unenrolled and unlicensed paid tax return preparers, Congress should enact the Administration's proposal to provide the agency with explicit authority to require all paid preparers to have a minimum knowledge of the tax code. Requiring all paid preparers to keep up with changes in the Code would help promote high quality services from tax return preparers, improve voluntary compliance, and foster taxpayer confidence in the fairness of the tax system. It would allow the IRS to focus resources on the truly fraudulent returns.

- ***Expanded access to National Directory of New Hires***. Under current law, the IRS is permitted to access the Department of Health and Human Services' National Directory of New Hires for purposes of enforcing the Earned Income Tax Credit and verifying employment reported on a tax return. The proposal would allow IRS access to the directory for broader tax administration purposes, which could assist the agency in preventing stolen identity refund fraud.

There are a number of other legislative proposals in the Administration's FY 2016 Budget that would also assist the IRS in its efforts to combat identity theft, including: giving Treasury and the IRS authority to require or permit employers to mask a portion of an employee's SSN on W-2s, which would make it more difficult for identity thieves to steal SSNs; adding tax-related offenses to the list of crimes in the Aggravated Identity Theft Statute, which would subject criminals convicted of tax-related identity theft crimes to longer sentences than those that apply under current law; and adding a $5,000 civil penalty to the Internal Revenue Code for tax-related identity theft cases, to provide an additional enforcement tool that could be used in conjunction with criminal prosecutions.

Senator Ayotte, this concludes my statement. I would be happy to take questions.