WRITTEN TESTIMONY OF
JOHN A. KOSKINEN
COMMISSIONER
INTERNAL REVENUE SERVICE
BEFORE THE
SENATE COMMITTEE ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS
ON UNAUTHORIZED ATTEMPTS TO ACCESS TAXPAYER DATA
JUNE 2, 2015

Chairman Johnson, Ranking Member Carper and Members of the Committee, thank you for the opportunity to appear before you today to provide information on the recent unauthorized attempts to obtain taxpayer data through the IRS's "Get Transcript" online application.

While we are continuing our in-depth analysis of what happened, the analysis thus far has found that the unauthorized attempts to request information from the Get Transcript application were complex and sophisticated in nature. These attempts were made using taxpayers' personal information already obtained from sources outside the IRS – meaning the parties making the attempts had enough information to clear the Get Transcript application's multi-step authentication process.

For now, our biggest concern is for the affected taxpayers, to make sure they are protected against fraud in the future. We recognize the severity of the situation for these taxpayers, and we are doing everything we can to help them.

Securing our systems and protecting taxpayers' information is a top priority for the IRS. Even with our constrained resources as a result of cuts to our budget totaling $1.2 billion since 2010, we continue to devote significant time and attention to this challenge. At the same time, it is clear that criminals have been able to gather increasing amounts of personal data 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 stolen from sources outside the IRS to perpetrate tax refund fraud exploded from 2010 to 2012, and for a time overwhelmed law enforcement and the IRS. Since then, we have been making steady progress, both in terms of protecting against fraudulent refund claims and prosecuting those who engage in this crime. Over the past few years, almost 2,000 individuals were convicted in connection with refund fraud related to identity theft. 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.

Additionally, as our processing filters have improved, we have also been able to stop more suspicious returns at the door, rather than accepting them for processing. This past filing season, our fraud filters stopped almost 3 million fraudulent returns before processing them, an increase of over 700,000 from the year before. But, even though we have been effective at stopping individuals perpetrating these crimes, we find that we are dealing more and more with organized crime syndicates here and around the world.

At the same time, over the last several years, the IRS has been working to meet taxpayers' increasing demand for self-service and electronic service options by providing them with more web-based tools, to make their interactions with us simpler and easier. As part of that effort, we launched the Get Transcript online application in January 2014. Get Transcript allows taxpayers to view and print a copy of their prior-year tax information, also known as a transcript, in a matter of minutes. Prior to the introduction of this online tool, taxpayers had to wait five to seven days after placing an order by phone or by mail to receive a paper transcript by mail. Taxpayers use tax transcript information for a variety of financial activities, such as verifying income when applying for a mortgage or student loan.

To access Get Transcript, taxpayers must go through a multi-step authentication process to prove their identity, consistent with many organizations in the financial services industry. They must first submit personal information such as their Social Security number (SSN), date of birth, tax filing status, and home address, as well as an email address. The taxpayer then receives an email from the Get Transcript system containing a confirmation code that they enter to access the application and request a transcript. Before the request is processed, the taxpayer must respond to several "out-of-wallet" questions – a customer authentication method that is standard within the financial services industry. The questions are designed to elicit information that only the taxpayer would normally know, such as the amount of their monthly mortgage or car payment.

During the 2015 filing season, taxpayers used the Get Transcript application to successfully obtain approximately 23 million copies of their recently filed tax information. If this application had not existed and these taxpayers had to call or write us to order a transcript, it would have stretched our limited resources even further. That is important to note, given our limitations during the past filing season. We would have been much less efficient in providing taxpayer service, not to mention the additional burden placed on taxpayers.

During the middle of May, our cybersecurity team noticed unusual activity on the Get Transcript application. At the time, our team thought this might be a "denial of service" attack, where hackers try to disrupt a website's normal functioning. Our teams worked aggressively to look deeper into the situation during the

following days, and ultimately uncovered questionable attempts to access the Get Transcript application.

As a result, the IRS shut down the Get Transcript application on May 21. The application will remain disabled until the IRS makes modifications and further strengthens security for the application. It should be noted that the third parties who made these unauthorized attempts to obtain tax account information did not attempt to gain access to the main IRS computer system that handles tax filing submissions. The main IRS computer system remains secure, as do other online IRS applications such as "Where's My Refund?" Unlike Get Transcript, the other online applications do not allow taxpayers to access their personal tax data.

As they continued to investigate, our team determined that a total of approximately 200,000 suspicious attempts to gain access to taxpayer information on the Get Transcript application had been made between mid-February and mid-May. About 100,000 of the attempts were unsuccessful, with the parties making these attempts unable to work their way through the protections in place.

But we know that the other 100,000 or so attempts to request information from the Get Transcript application between mid-February and mid-May were successful. We are analyzing what, if anything, was done with the personal information of these taxpayers obtained using the Get Transcript application, and have discovered the following:

- About 35,000 taxpayers had already filed their 2014 income tax returns before the unauthorized attempts at access. This means that these taxpayers' 2014 returns and refund claims were not affected by this fraudulent activity, because any fraudulent return subsequently filed in their names would be automatically rejected by our systems;
- For another 33,000, there is no record of any return having been filed in 2015. This could be the case for a number of reasons. For example, the SSNs associated with these individuals may belong to those who have no obligation to file, such as children, or anyone below the tax filing threshold;
- Unsuccessful attempts were made to file approximately 23,500 returns. These 23,500 returns were flagged by our fraud filters and stopped by our processing systems before refunds were issued; and
- Since this activity occurred, about 13,000 suspect returns were filed for tax year 2014 for which the IRS issued refunds. Refunds issued for these 13,000 suspect returns totaled about $39 million, and the average refund was approximately $3,000 per return. We are still determining how many of these returns were filed by the actual taxpayers and which were filed using stolen identities. We will work with any of these affected taxpayers who had fraudulent returns filed in their name.

As I mentioned at the outset, our analysis thus far has found that the unauthorized attempts to access information using the Get Transcript application were complex and sophisticated in nature. These attempts were made using personal information already obtained from sources outside the IRS – meaning the parties making the attempts had enough information to clear the Get Transcript application's multi-step authentication process, including answers to the out-of-wallet questions.

We believe it is possible that some of the attempts to access tax transcripts were made with an eye toward using the information to file fraudulent tax returns next year. For example, any prior-year return information criminals obtain would help them more easily craft seemingly authentic returns, making it more difficult for our filters to detect the fraudulent nature of the returns.

As noted above, since we have already disabled Get Transcript, our biggest concern right now is for the affected taxpayers, to make sure they are protected against fraud in the future. We recognize the severity of the situation for these taxpayers, and have taken a number of immediate steps to assist the affected taxpayers in protecting their data against fraud that might be perpetrated against them. First, we have placed an identifier on the accounts of the roughly 200,000 affected taxpayers on our core tax account system to prevent someone else from filing a tax return in their name – both now and in future years.

Second, we are in the process of writing to all 200,000 taxpayers to let them know that third parties appear to have gained access from outside the IRS to personal information such as their SSNs, in an attempt to obtain their tax information from the IRS. Although half of this group did not actually have their transcript accessed because those who were trying to gain this information failed the authentication tests, the IRS believes it is important to make these taxpayers aware that someone else has their personal data. We want them to be able to take steps to safeguard their data.

Letters have already been sent to all of the approximately 100,000 taxpayers whose tax information was successfully obtained by unauthorized third parties. We are offering credit monitoring, at our expense, to this group of taxpayers. We strongly encourage people who receive this letter to take advantage of this offer. We are also giving them the opportunity to provide us with the authentication documentation necessary to obtain an Identity Protection Personal Identification Number (IP PIN). This will further safeguard their IRS accounts and help them avoid any problems filing returns in future years.

As further analysis is done, we may uncover evidence that personal information of others, such as spouses and dependents of the taxpayers already identified, was also compromised, and we will take similar steps to protect those individuals.

More broadly, the IRS continues to work to help taxpayers who have been victims of identity theft. For example, for the 2015 filing season, the IRS has 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. Meanwhile, taxpayers living in Florida, Georgia and Washington, D.C. – three areas where there have been particularly high concentrations of identity-theft related 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.

In terms of our investigative work on identity theft, it is important to note that our Criminal Investigation (CI) division has seen an increase in identity theft crime being perpetrated by organized crime syndicates. The IRS is working closely with law enforcement agencies in the U.S. and around the world to prosecute these criminals and protect taxpayers. But the fact remains that these cyber criminals are increasingly sophisticated enemies, with access to substantial volumes of data on millions of people.

For that reason, we recently held a sit-down meeting with the leaders of the tax software and payroll industries and state tax administrators, and agreed to build on our cooperative efforts of the past and find new ways to leverage this public-private partnership to help battle identity theft. The working groups that were formed out of this meeting have continued to meet, and later this month we expect to announce an agreement on short-term solutions to help better protect personal information in the upcoming tax filing season, and to continue to work on longer-term efforts to protect the integrity of the nation's tax system.

One of the three working groups formed out of this meeting focuses on authentication. As criminals obtain more personal information, authentication protocols need to 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, our enemies in this area.

Congress has an important role to play here. Congress can help by approving the President's FY 2016 Budget request, which includes $101 million specifically devoted to identity theft and refund fraud, plus $188 million for critical information technology infrastructure. Along with providing adequate funding, lawmakers can help the IRS in the fight against refund fraud and identity theft by passing several important legislative proposals in the President's FY 2016 Budget proposal. A key item on this list is a proposal to accelerate information return filing 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 when copies of this information are provided to the taxpayers, generally by January 31 of the year following the year for which the information is being reported, which would assist the IRS in identifying fraudulent returns and reduce refund fraud related to identity theft.

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.

Chairman Johnson, Ranking Member Carper and Members of the Committee, thank you again for the opportunity to provide information on the recent unauthorized attempts to obtain taxpayer data through the IRS' Get Transcript online application. This concludes my statement, and I would be happy to take your questions.