



FOR IMMEDIATE RELEASE

June 2, 2015

CONTACT: [Aaron Fobes](#) , [Julia Lawless](#)

(202) 224-4515

Hatch Statement at Finance Hearing on IRS Data Theft

WASHINGTON – Senate Finance Committee Chairman Orrin Hatch (R-Utah) today delivered the following opening statement at a committee hearing regarding the data theft at the Internal Revenue Service (IRS) which compromised the private information of over 100,000 taxpayers:

Our hearing today concerns recent revelations that the Internal Revenue Service was the target of an organized service breach aimed at roughly 200,000 taxpayer accounts. We understand that over 100,000 of these breaches were successful, with cybercriminals obtaining confidential taxpayer information from the agency’s Get Transcript application.

In dealing with this breach here in the Senate, this Committee stands alone, having legislative jurisdiction over the Internal Revenue Code, oversight jurisdiction over the IRS, and wide-ranging abilities to conduct investigations dealing with individual taxpayer information.

While I have raised questions in the past about the way the IRS prioritizes its spending, today’s hearing is about finding out how criminals stole vast amounts of taxpayer information. Any questions regarding funding levels for the agency should wait until we have a complete understanding about what occurred.

Before we turn to the technological issues, let’s focus for a moment on the victims. Because of this breach, criminals were able to get personal information about roughly 104,000 taxpayers, potentially including Social Security numbers, bank account numbers, and other sensitive information. These taxpayers, and their families, must now begin the long and difficult process of repairing their reputations. And they must do so with the knowledge that the thieves who stole their data will likely try to use it to perpetrate further fraud against them.

Commissioner Koskinen, put simply, your agency has failed these taxpayers.

This hearing is of utmost importance as we work to find out what individuals and organizations were behind this breach; discover how this breach occurred, and what steps the IRS might have taken to prevent it; find out what taxpayer information was compromised, and how this may affect both taxpayers and tax administration going forward; and determine what

tools and resources are necessary to better protect taxpayers, catch cybercriminals, and prevent this type of breach from being successful in the future.

Most of all, we must pledge to work together to make sure that this type of breach does not happen again.

The secure movement of information is the lifeblood of international commerce and a necessary predicate for efficient government administration. Unfortunately, this information is also highly valuable to criminals.

We see it in the headlines nearly every week – a major insurance company, bank, or retailer, has its information security compromised and personal information or corporate data is stolen. Federal departments – especially defense related agencies – come under attack each and every day.

The IRS is not, and will never be, exempted from this constant threat.

In fact, there is reason to believe the IRS will be more frequently targeted in the future. After all, the IRS stores highly sensitive information on each and every American taxpayer, from individual taxpayers to large organizations and from mom and pop businesses to multinational corporations. The challenge of data security matters a great deal to every single taxpayer and will continue to be a central challenge to tax administration in the coming years.

Of course, data security and the protection of taxpayer information is of the highest importance in the prevention of stolen identity refund fraud. Identity theft, and the resulting tax fraud, costs taxpayers billions of dollars every year, and, once it occurs, it can take months or years for a taxpayer to mitigate the damage.

It was out of concern over stolen identity refund fraud that Ranking Member Wyden and I quietly launched an investigation earlier this year, requesting information and documents from the country's largest tax return preparers and debit card companies.

We look forward to working with the IRS as we move forward with this investigation and consider policy changes. We also look forward to hearing the report from your preparer working groups, and the committee looks forward to weighing in on those matters in the near future.

So I welcome our witnesses today, IRS Commissioner Koskinen and Inspector General George. Commissioner Koskinen, earlier this year, when I first welcomed you before the Committee as Chairman, I noted that I hoped it would be the beginning of a new chapter in the long, historic relationship between the Internal Revenue Service and the Senate Finance Committee. I said that because the issues before us are too great for that relationship to be anything but open, honest, and productive.

Today's topic is a great example of why that relationship is so important. Cyber threats will only continue to grow and those types of threats go to the core of our voluntary tax system. We must work together to figure out what happened, what went wrong in allowing the breach to occur, and how we can prevent another successful attack from taking place in the future.

Finally, I would like to acknowledge that today's hearing occurs during somewhat unusual circumstances.

The issue before us is the subject of several recently-opened investigations, including a criminal investigation conducted by TIGTA. I caution members of the committee to be sensitive to these investigations when asking questions of the witnesses, and be aware that they may not be able to provide full answers to every question in this public forum. In spite of these limitations, it is important to discuss this matter today as fully and candidly as possible.

###