

Ways and Means Subcommittees on Oversight and Social Security
QFRs
Hearing on Identity Theft and Tax Fraud
May 8, 2012

1. How can the Internal Revenue Service (IRS), the U.S. Treasury Inspector General for Tax Administration, and other law enforcement work to catch criminals sooner? Are there additional tools that you need which would require legislative action?

The IRS has taken aggressive measures to improve its filters and processes in an effort to prevent identity theft tax fraud on the front end of the tax filing process. In January 2012, the IRS's Criminal Investigation (CI) established a specialized unit to work almost exclusively on identity theft leads. This unit, known as the Identity Theft Clearinghouse (ITC), is comprised of two working groups within the North Atlantic Scheme Development Center (SDC). The ITC receives all refund fraud related identity theft leads from IRS-CI field offices. The ITC's primary responsibility is to develop and refer identity theft schemes to the field offices, facilitate discussions between field offices with multi-jurisdictional issues, and to work with the other SDCs to provide support for on-going IRS criminal investigations involving identity theft.

One way in which CI has proactively reached out to other law enforcement agencies is via a law enforcement alert bulletin that was developed and distributed to all CI field offices to share with their law enforcement partners. This bulletin helps law enforcement officers identify signs of identity theft related refund fraud and provides a local CI field office point of contact to assist. CI field offices have frequent contact with other federal law enforcement as well as state and local law enforcement in an effort to identify and address new trends in tax crimes. Additionally, Criminal Investigation continues to work closely in many states around the nation with multi-agency task forces designed to identify and disrupt identity theft related crime. These task forces pool resources to more quickly address identity theft allegations and allow for a more concentrated focus on combating identity theft related crimes.

The IRS also initiated a pilot program in the state of Florida to assist state and local law enforcement in identity theft investigative efforts. Through this pilot, identity theft victims can authorize the release of tax information on their accounts to Florida law enforcement authorities. Such information has allowed the participating agencies to obtain tax return information submitted by fraudsters to assist in their investigations of identity theft crimes.

Increasingly, the proceeds of identity theft and tax fraud, including tax refunds obtained by identity theft or fraud, are delivered onto prepaid devices, such as a prepaid card. The prepaid card industry, through the Prepaid Association Fraud Forum, is currently working with the IRS and Treasury/FMS to create a special "DD" rejection code for the prepaid card industry that suggests possible tax fraud that the IRS and Treasury/FMS can then tag as a high risk return.

Additionally, on July 29, 2011, the Financial Crimes Enforcement Network (FinCEN) issued final regulations for the prepaid access industry under the Bank Secrecy Act (BSA) that will assist in the early detection of this type of fraud. These regulations require the prepaid access industry to implement a comprehensive anti-money laundering framework which includes the filing of suspicious activity reports, collection and retention of customer and transactional information, and customer identification. Through the application of the BSA regulations, the prepaid providers and sellers will be in a better position to identify and report on cases of identity theft and tax fraud. This will provide the IRS and law enforcement with additional leads. Furthermore, the increased communication between IRS, other law enforcement agencies and the prepaid access industry should help in developing typologies and patterns so that industry and law enforcement can proactively recognize, prevent, and report on identity theft and tax fraud.

Two additional tools requiring legislative action would further assist us in combating identity theft. First, expanded access to information in the National Directory of New Hires which contains wage and unemployment insurance data, would improve the IRS's ability to identify fraudulent returns claiming fraudulent refunds, including, but not limited to, fraudulent refunds claimed by identity thieves. Second, reinstatement of the provisions under section 6103(k)(10) of the Internal Revenue Code authorizing the IRS to disclose return information with respect to individuals incarcerated in Federal or State prisons whom the IRS determined may have filed or facilitated the filing of a false return would allow the IRS to combat tax fraud from identity theft committed by prisoners. This authorization expired on December 31, 2011. Both of these tools are included in the tax proposals of the Administrations' FY 2013 Budget. Additionally, the President's FY2013 Budget proposes an amendment to the BCA to permit program integrity cap adjustments in support of additional IRS investments. The Budget request includes a total program integrity cap adjustment of \$691,028,000 in additional appropriation for tax enforcement and compliance activities. These new initiatives are projected to generate more than \$1.48 billion in additional enforcement revenue annually once the resources are fully mature.

2. Should state and local law enforcement have access to taxpayer information, such as refund data, in pursuing identity theft cases? Why or why not?

As noted in the response to the previous question, the IRS has commenced a pilot program in the state of Florida that provides a means for state and local law enforcement to access just such data. This pilot program is still underway. The results will be analyzed in the coming months. As part of this analysis, the IRS will review whether the tax return information is beneficial to state and local law enforcement. The IRS will also analyze what additional resources would be required to sustain and/or expand the program.

3. Law enforcement and federal prosecutors make decisions on what cases to pursue based on competing priorities and varying levels of fraud. People hear of the \$130 million cases being pursued, but how much of this problem exists at lower levels- \$5,000 in fraud or \$20,000 in fraud- and are these cases vigorously pursued? Do prosecutors only get interested when fraud reaches the incredible levels we read about in newspapers?

While each case needs to be evaluated on its own merits, it is clear that not every instance of identity theft involving tax fraud can be addressed by a criminal prosecution. Resource constraints within IRS Criminal Investigation, competing prosecutorial priorities of the United States Attorney's Offices, as well as overall capacity issues in the Federal court system make it impossible to address every instance of identity theft related refund fraud criminally.

Generally speaking, it is the more egregious cases that receive priority. While egregiousness can be measured in part on dollar amount, the number and type of victims, and the actual tax loss sustained by the fraud scheme are also considered among other factors. In all instances, sufficient evidence must still be developed before a case can be successfully prosecuted.

The IRS believes that continued improvement to tax fraud filters and processes, combined with criminal investigation and prosecution at the state, local, and Federal levels, is the best way to reduce tax fraud from identity theft going forward.

4. You reported to the Senate Finance Committee's Subcommittee on Fiscal Responsibility and Economic Growth hearing that as of March 9, 2012, IRS had stopped 215,000 questionable returns with \$1.15 billion in claimed refunds from filters specifically targeting refund fraud. Can you tell us how much money has gone out the door due to fraud this year, or last year?

Historically, we have not tracked revenue loss in this manner due to systems limitations, but we are pursuing whether there is a means to aggregate the losses based on post-refund tax returns that we subsequently confirmed as fraudulent. Also, moving forward we are looking into developing a process to assess and calculate revenue lost due to tax fraud through identity theft. This will give us a better estimate of the revenue loss though not a complete picture.

5. Please tell us what the IRS is doing to further protect taxpayers from identity theft and tax fraud for next filing season. Will the IRS continue its collaboration with software developers, financial institutions and others to explore industry best practices and new innovations to better prevent theft for 2013?

We are implementing new processes for handling returns, new filters to detect fraud, and a continued commitment to investigate the criminals who perpetrate crimes. We will continue partnering with our stakeholders including software developers, financial institutions, the prepaid card industry, tax professionals, and other law enforcement agencies, etc. For victim assistance, the IRS is working to speed up case resolution, provide more training for our employees who assist victims of identity theft, and step up outreach to and education of taxpayers so they can prevent and resolve tax-related identity theft issues quickly. For example, we will implement a systemic locking mechanism that will prevent the filing of a tax return by an identity thief for certain taxpayer accounts, improve systemic capabilities, and expand the use of the Identity Protection PIN (IP PIN) and improve its functionality to validate returns using the IP PIN earlier in the e-file process. We have also streamlined the IP PIN replacement process for those taxpayers who have lost or misplaced their IPPIN. In addition, our ongoing Return Preparer Program, will aid in curbing identity theft by unscrupulous return preparers.

As stated in response to Question 1 above, there are additional tools requiring legislative action which would allow the IRS to better prevent fraudulent refunds from identity theft.