



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

DEPUTY COMMISSIONER

June 18, 2013

The Honorable Lois Frankel
U.S. House of Representatives
Washington, DC 20515

Dear Ms. Frankel:

Thank you for your inquiry dated February 19, 2013, requesting an update on the ways the IRS is combating refund fraud.

I share your concerns about identity theft and refund fraud and the negative effect they have on taxpayers and government agencies. As we have done in previous filing seasons, we developed and implemented a comprehensive identity theft strategy for the 2013 filing season that focused on preventing, detecting, and resolving identity theft cases as quickly as possible. We also have instituted a number of new procedures in the last few years to improve our ability to prevent tax refund fraud using stolen identities. Several of our efforts are highlighted below.

How is the IRS using the most advanced technology to help identify potentially fraudulent refund claims?

The Administration's Fiscal Year (FY) 2014 Budget request provides \$101 million to support the IRS's efforts to prevent identity theft-related refund fraud, protect taxpayers' identities, assist victims of identity theft, and enhance the revenue protection strategy implemented in FY 2013. The increase in funding will support the development and implementation of technology enhancements to identify noncompliant returns before refunds are issued, manage and track workload and case results, send notification letters to taxpayers, and allow third-party data to be used earlier in the filing season. This enhancement will improve detection of fraudulent returns and reduce delays of legitimate refunds due to pre-refund compliance activities.

In FY 2013, we significantly increased the number and accuracy of filters that detect potential identity theft before we issue refunds. We stopped five million returns claiming \$20 billion in fraudulent refunds in FY 2012, up from three million returns claiming \$14 billion in FY 2011. This fiscal year, through April 30, 2013, we have stopped more than 600,000 returns claiming \$3.6 billion in fraudulent refunds. We created and revised several technological tools to help employees perform research and resolve identity theft cases more efficiently. We have issued more than 770,000 Identity Protection

Personal Identification Numbers (IP PIN) for the 2013 tax season, up from about 250,000 for tax year 2011, to protect more tax accounts of more identity theft victims.

Does the IRS employ interoperable computer systems, so that all departments within the IRS can share the same data, flag potential problems and resolve conflicts in the most efficient timeframe possible?

The IRS utilizes its Masterfile and Integrated Data Retrieval System to notate identity theft activity on a taxpayer's account. It also screens returns for fraud at multiple stages in the processing life-cycle using a variety of internal systems including the Electronic Fraud Detection System, Return Review Program, and Dependent Database. In 2008, we began placing indicators on the accounts of taxpayers who have experienced identity theft. These indicators alert employees across the IRS that a taxpayer has been identified as a victim of identity theft. The indicators also speed up account reconciliation for the legitimate taxpayer and reduce the likelihood that a taxpayer's information could be used for a fraudulent refund claim in subsequent years. As our identity theft indicator program has developed, we have leveraged it to put in place additional proactive tools that identify fraudulent returns at the point of filing.

Additionally, all of the IRS's specialized identity theft groups' applications have links to identity theft resources that provide the latest information. Our IRS-wide information page provides daily alerts on any changes in processing and alerts on refund schemes. We broadened the scope of our employee training to require all employees who might interact with an identity theft victim to take an awareness briefing that includes significant procedural developments, as well as knowledge checks for each key objective. About 37,000 employees completed this training in advance of the 2013 filing season. We realigned some of our departments to bring together the functions responsible for revenue protection, refund compliance, and taxpayer correspondence. We established IRS-wide liaisons for identity theft issues and implemented a referral program for employees to refer cases with the potential for refund fraud.

How is the IRS coordinating with the Social Security Administration, the Department of Justice, and other relevant federal agencies to combat refund fraud?

In January 2013, the IRS, in a joint effort with the Department of Justice (DOJ) and local U.S. Attorneys' offices, conducted a national sweep targeting identity theft suspects in 32 states and Puerto Rico, which involved 215 cities and their surrounding areas. The coast-to-coast effort against 389 identity theft suspects led to 734 enforcement actions in January, including indictments, complaints, and arrests. The effort comes on top of a growing identity theft effort that led to 2,400 other enforcement actions against identity thieves during FY 2012.

We recently expanded to all 50 states, as well as the District of Columbia, the law enforcement waiver pilot that started in Florida in 2012. More than 1,560 waiver requests have been received since the Law Enforcement Assistance Program's inception from over 100 state and local law enforcement agencies in the nine states

participating in the pilot. The expansion to all 50 states will enable taxpayers to sign a waiver allowing us to disclose their tax information to help local authorities investigate and prosecute tax-related identity theft cases. The national effort with the DOJ and other federal, state, and local agencies is part of our comprehensive identity theft strategy.

The IRS Criminal Investigation (CI) division expanded its efforts during January 2013, pushing the total number of identity theft investigations to more than 1,460 since the start of FY 2012. In addition to the criminal actions, IRS auditors and criminal investigators conducted a special compliance effort that started in January 2013, to visit 197 money service businesses to help ensure these businesses are not perpetuating identity theft or refund fraud when they cash checks. The compliance visits occurred in 17 high-risk locations covering areas in and surrounding New York, Philadelphia, Atlanta, Tampa, Miami, Chicago, Houston, Phoenix, Los Angeles, San Diego, El Paso, Tucson, Birmingham, Detroit, San Francisco, Oakland, and San Jose.

In response to the growing threat that identity theft poses to tax administration, the IRS established the Identity Theft Clearinghouse (ITC), a specialized unit within CI that became operational in 2012, to work on identity theft leads. The ITC receives all refund fraud-related identity theft leads from 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 provide support to ongoing criminal investigations involving identity theft.

In January 2013, IRS CI hosted an Identity Theft Summit in Washington, DC. Law enforcement officers from 14 partnering federal agencies met to discuss ways to strengthen collaborative efforts among agencies in the fight against identity theft.

The IRS is also collaborating with the Social Security Administration and other parts of the Administration on a potential legislative change to restrict access to the Death Master File (DMF) to those users who legitimately need the information for fraud prevention purposes and to delay the release of the DMF for 3 years to all other users. This change would make it more difficult for identity thieves to obtain identifying information of deceased persons in order to file fraudulent returns.

In what ways is the IRS facilitating a single point of contact for victims of identity theft in the event that victims must interact with multiple units at the IRS?

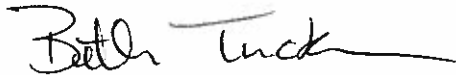
In October 2012, we established several identity theft specialized groups to assist the pre-existing Identity Protection Specialized Unit (IPSU) with processing identity theft cases for the 2013 filing season. These groups will provide a single point of contact, i.e., entry point to the IRS, for victims based on origin of the problem. If the taxpayer has only one identity theft-related issue, then the IRS employee who is assigned to work the case is his/her single point of contact. For victims that have multiple issues crossing functions, their cases continue to be monitored by the IPSU, and they will be given the IPSU number as their single point of contact. We more than doubled staffing resources

dedicated to working identity theft cases this year. We now have more than 3,000 employees working identity theft issues. In all identity theft situations, our employees work with each victim to resolve his/her particular situation. Identity theft cases are becoming increasingly complex, involving a manual authentication and review process to ensure we resolve the case satisfactorily for the victim. We are working to speed up case resolution, provide more training for our employees who assist victims of identity theft, and increase outreach to and education of taxpayers and tax return preparers so they can prevent and resolve tax-related identity theft issues quickly.

Stopping identity theft and refund fraud is a top priority for the IRS. Our work on identity theft and refund fraud continues to grow, touching nearly every part of our organization. We will continue to respond to this challenge and find ways to detect and prevent identity theft and fraud within the tax system.

If you have any further questions, please contact me or a member of your staff may contact Catherine Barré, Director, Legislative Affairs, at (202) 622-3720.

Sincerely,

A handwritten signature in black ink, appearing to read "Beth Tucker", with a long horizontal flourish extending to the right.

Beth Tucker
Deputy Commissioner for
Operations Support

Congress of the United States
House of Representatives
Washington, DC 20515-0922

February 19, 2013

Steven T. Miller
Acting Commissioner
Internal Revenue Service
U.S. Department of the Treasury
1111 Constitution Avenue, NW, Room 3241
Washington, DC 20224

RECEIVED

By Executive Secretariat at 12:25 pm, Feb 20, 2013

Dear Acting Commissioner Miller:

I recently learned about an alarming new tax fraud scam being perpetrated on unsuspecting taxpayers. According to an NPR story that aired on February 18, criminals are stealing Social Security numbers and submitting fraudulent income tax returns to unlawfully claim the corresponding refunds. When real tax filers seek their refunds, they find that criminals have already claimed it, and the victims must wait months or even a year to receive the refund that is rightfully theirs.

The scope of the refund fraud is staggering. According to the National Taxpayer Advocate, refund fraud cases have increased by about 650 percent since 2008. Regrettably, South Florida appears to be the epicenter for this tax fraud epidemic. In my short time as a Member of Congress, I have already received three cases of Social Security identity theft, including one constituent who had his identity stolen three times and now cannot obtain a new Social Security Card.

Each refund fraud case contributes to the loss of much-needed federal revenues. One official with the Treasury Department estimated that the fraud scam could cost the federal government \$21 billion over the next five years. At a time when Congress and the President are grappling with how to balance our federal budget, we simply cannot let these important tax revenues fall into the hands of criminals.

To this end, I respectfully request an update on ways the IRS is combatting refund fraud, including responses to the following questions:

- How is the IRS using the most advanced technology to help identify potentially fraudulent refund claims?

- Does the IRS employ interoperable computer systems, so that all departments within the IRS can share the same data, flag potential problems and resolve conflicts in the most efficient timeframe possible?
- How is the IRS coordinating with the Social Security Administration, the Department of Justice, and other relevant federal agencies to combat refund fraud?
- In what ways is the IRS facilitating a single point of contact for victims of identity theft in the event that victims must interact with multiple units at the IRS?

With the tax filing season underway, I trust that you will respond to my request in a timely fashion, and I look forward to working with you on this and future issues to ensure that the Internal Revenue Service is best serving the needs of the American public.

Sincerely,

A handwritten signature in black ink, reading "Lois Frankel". The signature is fluid and cursive, with the first name "Lois" and last name "Frankel" clearly distinguishable.

Lois Frankel
Member of Congress

cc: Catherine Barre, Director of Legislative Affairs