
2011

# Fraudulent Returns
# Revenue Protection and Victim Assistance

David Knight
Director, Pre-Refund Program
EITC Office
ETA & Refundable Credits
Wage & Investment Division

# Refund Fraud: Revenue Protection Numbers

- Since 2009, IRS has blocked +/-$925M in refunds to identity thieves
- In filing season 2011, IRS found over $500M of false refunds claimed by prisoners, representing +/- 225% more than in filing season 2010.
- Although IRS is able to detect large volumes of fraudulent and non-compliant refunds, “we do not know what we do not know.”

2011

Internal Revenue Service SDC Software Developers Conference

# Refund Fraud: ID Theft Victim Numbers

- In 2010, government / benefits fraud related to taxes or wages overtook credit card fraud as most common form of identity theft as per Federal Trade Commission (FTC).
- Since 2009, IRS has received 100K paper cases and provided over 265K telephone services
- In 2010, IRS provided telephone services to 175K callers with ID Theft issues.
- IRS has implemented eight unique identity theft indicators to mark taxpayer accounts and help resolve identity theft-related tax account issues. To date, over 470K incidents of identity theft have been identified, impacting more than 350K taxpayers.

# Refund Fraud: Identity Theft Scenarios

- Refund-Related Identity Theft
  - An identity thief uses a legitimate taxpayer's identity to fraudulently file a tax return and claim a refund. Generally, the identity theft perpetrator will use a stolen Social Security Number (SSN) to file a forged tax return and attempt to obtain a fraudulent refund early in the filing season.
  - The legitimate owner of the SSN may be unaware that this has happened until s/he files the return later in the filing season and it is discovered that two returns have been filed using the same SSN.

# Refund Fraud: Identity Theft Scenarios

- Employment-Related Identity Theft
  - An identity thief uses someone else's name and SSN in the process of obtaining a job. In this situation, the identity thief's employer will report the employee's wage information to the IRS, just as the legitimate taxpayer's employer reports his legitimate wages.
  - However, if the legitimate taxpayer is unaware that an identity thief is using his SSN for employment, the IRS may conclude that he has not properly reported all earned income and a notice of unreported / underreporting income would be generated and sent to the taxpayer. As a result, the legitimate taxpayer must work with the IRS to resolve his account issues and obtain an identity theft marker on his account.

# Combating Revenue Loss from Refund Fraud

- IRS has made significant progress in building its organizational resources to fight refund fraud.
- In July 2006, IRS created the Pre-Refund Program to extend detection and resolution of false refunds BEFORE they are released and to minimize harm to good taxpayers.
- In July 2007, IRS created the Office of Privacy, Information Protection and Data Security (PIPDS) to provide a centralized privacy program and implement standardized identity theft processes across all IRS organizations.

2011

# Combating Revenue Loss from Refund Fraud

- In October 2009, IRS created the Taxpayer Assurance Program (AMTAP) to screen and verify questionable information returns. In filing season 2011, AMTAP doubled the number of prisoner returns screened to 200,000.
- In 2010, IRS stood up a new program to combat prisoner tax fraud and non-compliance.

2011

Internal Revenue Service SDC Software Developers Conference

# Combating Revenue Loss from Refund Fraud

- The Criminal Investigation (CI) Division plays a vital role in responding to refund fraud. CI investigates and detects tax fraud and other financial-related fraud, including identity theft.
- 2010: CI investigated 41 identity theft schemes of national scope were investigated by CI,
- In 2010, 95 percent of individuals who DOJ prosecuted for refund-related identity theft went to prison.
- 2011: California woman sentenced to 30 months in prison, three years of supervised release, and was ordered to pay more than $800,000 in restitution for participating in such a scheme to defraud the IRS.

2011

Internal Revenue Service SDC Software Developers Conference

# Assisting Victims of ID-Theft-Related Refund Fraud

- In 2008, IRS established the Identity Protection Specialized Unit (IPSU) to address initial taxpayer inquiries about identity theft. The unit provides a dedicated toll-free number, staffed by English and Spanish-speaking IRS employees.
- IRS also established an online fraud program to shut down web sites and phishing sites posing as the IRS or legitimate e-file providers. Since FY 2009, we shut down 8,296 sites.
- IRS partnered with the Internet Crime Complaint Center (IC3), a federal working group collaborating on Internet crimes investigations, including identity theft.

# Stretching Resources

- IRS has built its organizational capacity to combat refund fraud and assist victims.
- IRS is taking steps in FS2012 to protect more revenue and provide more assistance to victims
- IRS' future state vision includes up-front electronic matching of third-party data, risk algorithms, the opportunity to self-correct, and a hierarchy of more automated treatments to stretch the capacity of IRS resources and allow them to focus on problem areas such as refund fraud.

# New Revenue Protection Capabilities

- New systemic capabilities to detect repeat instances of identity theft.
- New application that will further assist the IRS in identifying prisoners and resolving false claims
- Testing ability to lock down accounts for SSNs with no filing obligation

# New Victim Assistance Capabilities

- January 2011, IRS began issuing victims an Identity Protection Personal Identification Number (IP PIN) to use when filing future returns.
- The IP PIN was piloted with +/-56K taxpayers, and 1040 series tax forms were revised to allow for entry of the IP PIN.
- The IP PIN should avoid delays in filing and processing Federal tax returns for taxpayers who have been verified by the IRS to be victims of identity theft.

# Commissioner's Vision: "Look-Forward" Compliance

- Current State: "Look-Back" Compliance
  - Risk modeled from past-year compliance data
  - IRS receives information returns, e.g., W-2, 1099 after taxpayer files return.
  - Audit usually occurs after refund is released
  - Audit can occur as many as three years after filing
  - Interest and penalties may have been accruing
  - Taxpayers who received undue refunds may no longer have money that was refunded incorrectly
  - Collection is expensive, and collectibility decreases with time

# Commissioner's Vision: "Look-Forward" Compliance

- Information returns available electronically before filing
  - IRS would get all information returns from third parties (W2s, 1099s, etc) before individual taxpayers filed.
  - Taxpayers or preparers could access via Web and download into returns using commercial tax software.
  - Taxpayers would add self-reported and supplemental information and file their tax returns with IRS.
  - IRS would embed third-party information into pre-screening filters and immediately reject any return for self-correction.
  - Risk models could be built using link analysis on a much more robust data set.

# Commissioner's Vision: "Look-Forward" Scenario

- Taxpayer mistakenly enters $2,000 in dividends on his return, but 1099's show $3,500.
- IRS follows up on discrepancy well after the return is filed to address the unreported income.
- In the Commissioner's "Look-Forward" vision, this scenario simply wouldn't occur.
  - Taxpayer would begin filing with access to all the information that has been reported to the IRS.
  - Taxpayers could resolve discrepancies between information as reported to the IRS and their own records before filing the tax return.

# Questions for You

- What fraud scenarios are we either missing or under-responding to?
- What recommendations do you have about the use of third-party data to validate the tax return?
- What ID Theft and fraud detection tools do you use?
- How can software developers assist IRS in combating fraud and minimizing customer risk?
- What risk factors do you look at, e.g., multiple refunds to a single account, first time filer, no filing obligation, etc?

# Thank You