


Criminal Investigation

Criminal Investigation



Stolen Identity Refund Fraud (SIRF)

<p>Nneka Sutherland (267) 941-6281</p>	<p>Special Agent Nneka.Sutherland@ci.irs.gov</p>
<p>Joseph Carl (267) 941-6117</p>	<p>Special Agent Joseph.Carl@ci.irs.gov</p>

IRS – Criminal Investigation

- Primary Investigative Jurisdiction
 - Criminal Tax Offenses (Title 26)
 - Money Laundering Crimes (Title 18 §§ 1956/1957)
 - Bank Secrecy Act Violations (Title 31)

- Tax Refund Crimes (Title 18 USC 287, 286, 1028)
 - Return Preparer Cases
 - Questionable Refund Cases
 - ID Theft Cases


Criminal Investigation

What is Identity Theft?

The unauthorized acquisition and use of a true person’s identity and personal information for unlawful purpose.

- Name
- Address
- Date of Birth
- Social Security number
- Credit card / bank numbers
- Mother’s maiden name
- Driver’s License Information



Criminal Investigation

Tax Refund Identity Theft

- Occurs when someone uses your personal information without your permission to file a tax return.
- The FTC estimates that as many as 9 million Americans have their identities stolen each year.

Criminal Investigation

How and When ID's are Stolen

Almost always from outside of IRS:

- Dumpster diving
- Skimming
- Phishing
- Address changes
- Theft of records
- Data breaches
- Trojan viruses
- Spyware



Criminal Investigation

The Players





Three General Groupings:

- ID Thieves
- Return Preparers
- Money People

Criminal Investigation

ID Thieves



- Steal **Personal Identifying Information (PII)** generally from their employer, place of business, or purchase off the street.
- Sell PII to co-conspirators.
- PII may be in the form of a business record or handwritten lists.

Criminal Investigation

Return Preparers



- Buy PII from the person who stole it.
- Return filer may be hard to identify.
- Use PII to prepare returns and control how refunds will be received:
 - Prepaid Access (PPA) card;
 - Treasury check;
 - Direct deposit; and/or
 - Refund Anticipation Loan (RAL).

Criminal Investigation

Money People



- Obtain the proceeds of the scheme.
- Can include people holding bank accounts (foreign students), apartment managers, checks cashers, and store owners.
- People withdrawing funds from ATMs using PPA cards.



Charges in SIRF Cases

- 18 U.S.C. § 286/287 (False Claims)
- 18 U.S.C. § 641 (Theft of gov't funds)
- 18 U.S.C. § 1029 (Access device fraud)
- 18 U.S.C. § 1343 (Wire fraud)
- 18 U.S.C. § 1028 (ID theft)
- 18 U.S.C. § 1028A (Aggravated ID theft)
- 18 U.S.C. § 371 (Conspiracy)



Partners in Law Enforcement

- SIRF schemes are commonly detected in one of three ways:
 1. Leads from Postal Service
 2. Local PD's make vehicle stops and find Treasury checks and/or tax documents not belonging to the vehicle occupants.
 3. Informants
 4. IRS-CI – Scheme Development Center



Partnering – Federal

- CI currently participates on joint investigations and collaborates with other Federal Agencies during task force settings and interagency working groups
- CI provides updated guidance to other Federal Agencies as to the proper procedures for returning proceeds of stolen refund fraud to the Department of the Treasury

Criminal Investigation

Partnering State/Local

- CI special agents throughout the country participate in at least 35 task forces and working groups with federal, state, and local law enforcement that target tax related identity theft crimes
- CI personnel also coordinate with these agencies in an effort to ensure that victims are aware of the steps they need to take to resolve their affected tax accounts
- IRS developed the Identity Theft Victim Disclosure Waiver Process

Criminal Investigation

SIRF Schemes

- Criminals use stolen identities to file false tax returns requesting refunds
- Usually, the false tax returns are filed early in the filing season (January-February)
- Victims are often unaware a false return has been filed in their name until their tax return is rejected when they attempt to E-file



Criminal Investigation

SIRF Schemes...

- Large fraudulent tax refund schemes may involve multiple individuals:
 - Organizer
 - ID Stealer
 - ID purchaser
 - Return preparer
 - Refund receiver
 - Check casher
- Gangs, drug dealers, organized crime have all moved into orchestrating tax refund schemes

Criminal Investigation

SIRF Schemes...

- Fraudulent tax refunds may be received at any time during the year
- Refunds from false tax returns usually received in one of three ways:
 - Paper check
 - Direct deposit into a bank account
 - Direct deposit onto a prepaid card



Criminal Investigation

False Paper Check Refunds

- Issued in the name of the ID Theft victim
- Often use generic addresses, such as:
 - PO Boxes
 - Hotels
 - Apartments
 - Shelters



Criminal Investigation

False Paper Check Refunds

Look for:



- Individuals in possession of multiple US Treasury checks
 - Tax refund checks usually say “Tax Refund” under the check # (right side)
- Be especially concerned if:
 - Checks list different payees, but same address
 - Checks are for similar amounts
 - Checks made out to individuals in other areas of country

Criminal Investigation

Prepaid Cards

What to Look for:

- Individuals with multiple prepaid cards, especially prepaid cards with tax preparation software branding (TurboTax, H & R Block, etc.)
- Lists of 16-digit “card” #'s with correlating “account” #'s



Criminal Investigation

Schemes Involving US Territories

- Most residents of US Territories (Puerto Rico, Guam, US Virgin Islands, etc.) are US Citizens and have Social Security Numbers

HOWEVER...

- Since income earned in US Territories is generally not subject to Federal taxes, they generally do not file income tax returns



Criminal Investigation

Schemes Involving US Territories

- Fraudsters often utilize the identifying information of residents of US Territories for SIFR schemes because they know the victim will not be filing a legitimate tax return.
- Because there is no legitimate tax return...
 - The false return can be filed any time of the year
 - The false return cannot be compared with prior legitimate returns to determine accuracy

 **Criminal Investigation**

Indications Someone's Identity May Have Been Stolen

They receive notification that:

- ... they filed more than one tax return or someone has already filed using their information.
- ... they receive notice from the IRS they have a balance due or refund pending for a year they did not file.

 **Criminal Investigation**

How SIRF Victims Should Respond

- Call the IRS Identity Protection Specialized Unit, toll-free at 1-800-908-4490 (7 AM – 7 PM)
- Either:
 - File a police report with local/state police; OR
 - Complete the IRS Identity Theft Affidavit (Form 14039) and compile requested documents
- Report the ID Theft to the FTC via www.consumer.gov/idtheft or (877) 438-4338

 **Criminal Investigation**

How SIRF Victims Should Respond

- Contact the fraud department of the three major credit bureaus:

Equifax – www.equifax.com	(800) 525-6285
Experian – www.experian.com	(888) 397-3742
TransUnion – www.transunion.com	(800) 680-7289

 

 **Criminal Investigation**

How Law Enforcement Should Respond to Potential SIRC

For urgent issues, call S/A Tyler Boyer (610)-861-5683, S/A Matthew McKenna (215) 861-1395 (or any IRS-CI agent) directly

- Important to provide information to IRS-CI for “deconfliction” purposes

 **Criminal Investigation**

Understanding the IRS Process

- The taxpayer attempts to file a return or experiences a loss of PII.
- IRS Form 14039, *Identity Theft Affidavit*, is filed.
- IRS codes taxpayer’s account to show identity theft documentation was submitted.
- IRS reconciles taxpayer’s account to reflect valid return information.
- Identity protection indicator is placed on the taxpayer’s account.

 **Criminal Investigation**

Understanding the IRS Process

- IRS issues a CP01 notice to let the taxpayer know an identity theft marker has been placed on his/her account.
- Before the next filing season, the IRS generally assigns the taxpayer a unique Identity Protection PIN to verify his/her return.
- If the taxpayer is identified as being deceased, the IRS locks the account to prevent future filing.



 **Criminal Investigation**

Local / State Law Enforcement

- Victims of SIRF should alert local and/or state law enforcement of the theft
- Local law enforcement may be able to receive tax information to assist them in prosecuting SIRF cases not worked by IRS-CI

 **Criminal Investigation**

**Assisting Financial Institutions
(External Leads Program)**

- The IRS is collaborating with more than 130 financial institutions to identify identity theft fraud schemes and block refunds
- This effort has protected hundreds of millions of dollars

 **Criminal Investigation**

Protect Yourself from ID Theft

- **Secure** personal information in your home
- **Don't** give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact or you are sure you know who you're dealing with.
- **Protect** your Social Security number.
- **Protect** personal computers: use firewalls, anti spam and virus software and update security patches.

 **Criminal Investigation**

Protect Yourself from ID Theft

- Beware of *Phishing*
- *Phishing* is the act of sending an e-mail to a user falsely claiming to be a legitimate enterprise in an attempt to scam the user into surrendering private information that could be used for identity theft.
- Don't click hyperlinks in emails.
- Don't click on pop-up windows on computers.
- Review web addresses to confirm where you are

 **Criminal Investigation**

Protect Yourself from ID Theft

Remember, the IRS does not request sensitive information by e-mail.

 **Criminal Investigation**

IRS Phone Scams

- Victims are told they owe money to the IRS and it must be paid promptly through a pre-loaded debit card or wire transfer.
- If the victim refuses to cooperate, they are then threatened with arrest, deportation or suspension of a business or driver's license. In many cases, the caller becomes hostile and insulting.

 **Criminal Investigation**

IRS Phone Scams

- Scammers use fake names and IRS badge numbers.
- Scammers may be able to recite the last four digits of a victim's Social Security Number.
- Scammers spoof the IRS toll-free number on caller ID to make it appear it's the IRS calling.
- Scammers sometimes send bogus IRS emails to some victims to support their bogus calls.

 **Criminal Investigation**

IRS Phone Scams

- Victims hear background noise of other calls being conducted to mimic a call site.
- After threatening victims with jail time or driver's license revocation, scammers hang up and others soon call back pretending to be from the local police or DMV, and the caller ID supports their claim.

 **Criminal Investigation**

IRS Phone Scams – What to Do

- If you think you may owe taxes, call the IRS toll-free number to see if the call is legitimate:
– 1-800-829-1040.
- If you are confident the call is a scam, call the Treasury Inspector General for Tax Administration (TIGTA) at 1-800-366-4484 to report the incident.
- Contact the FTC if portions of your identity appear to have been compromised.

Internal Revenue Service
Criminal Investigation

Protect Yourself from ID Theft

- **Review** your bank statements and credit card bills often.
- **Check** your credit report once every 12 months.
- **Request** a free annual copy of your credit report from www.annualcreditreport.com or call toll-free (877) 322-8228

Internal Revenue Service
Criminal Investigation

Any Questions??


