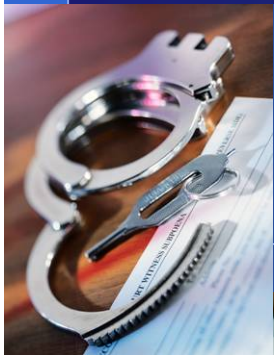


IRS Criminal Investigation

Detroit Field Office





Identity Theft

- ❖ The FTC estimates that as many as 9 million Americans have their identities stolen each year.





How Do They Get Your Information?

- ❖ Theft of valuables – purses, wallets, cell phones
- ❖ Dumpster dive – rummage through trash looking for receipts and statements
- ❖ Mail theft – change of address
- ❖ Business record theft – customer, student, employee or patient
- ❖ Posing as a landlord or employer to obtain credit reports
- ❖ Internet search – file sharing
- ❖ Fraudulent email – Phishing or Vishing
- ❖ Phone records
- ❖ Eavesdropping / “shoulder surfing”
- ❖ Trick you into revealing information – scams
- ❖ Skimming devices
- ❖ Just plain lacks with personnel information – unsecured sites, social media, open pages



Identity Theft

- ❖ How criminals use stolen personal information:
 - File fraudulent tax returns
 - Seek employment
 - Open/exploit financial accounts
 - Sell for a profit





What is Tax Refund Identity Theft

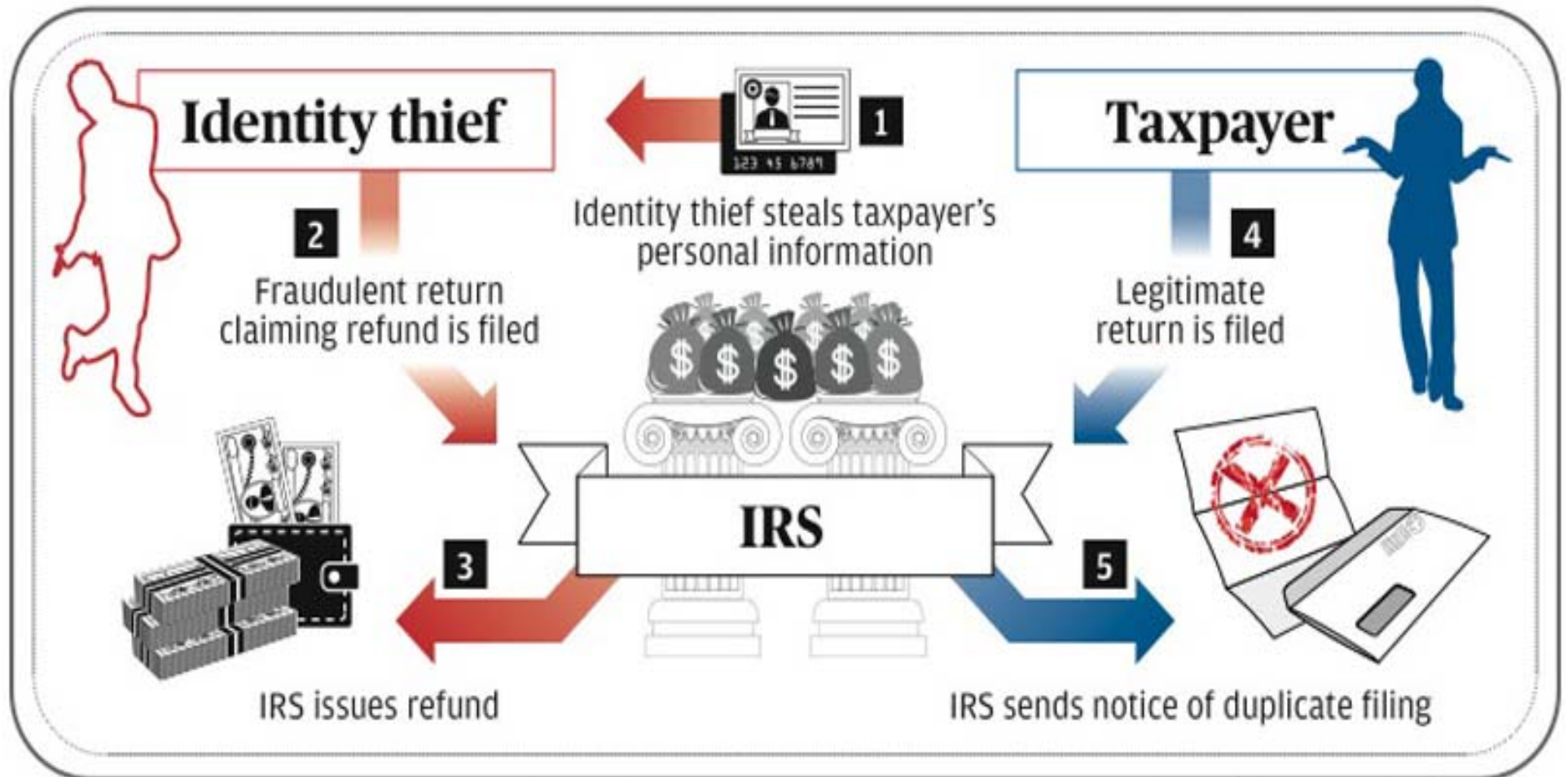


- ❖ Occurs when someone uses your personal information without your permission to file a tax return.



Stolen ID Refund Fraud

- What do I need to commit the crime?



Source: U.S. Government Accountability Office

Staff graphic by Gerald Fullam



Identity Theft: Current Trends

- ❖ Refund Schemes perpetrated by prisoners
- ❖ Stolen dependants for additional credits (EITC)
- ❖ Use of identity by prior year tax return preparer
- ❖ Use of identities of those not likely required to file a Federal tax return
- ❖ Use of non-wage and withholding tax returns (i.e. Interest Income, Schedule D, Schedule C)



Protect Your Personal Information

- ❖ Do not leave valuables unattended
- ❖ Keep your important papers secure – account numbers, passports, S/S cards, vehicle titles
- ❖ Review all statements regularly – check for unauthorized charges or suspicious activity. Close any unused or unauthorized accounts
- ❖ Be careful with your mail – locked boxes
- ❖ Shred sensitive documents
- ❖ Pick up new checks from your financial institution
- ❖ Utilize on-line bill pay and direct deposit of income
- ❖ Do not overshare on social networking sites
- ❖ Do not authorize payment over the phone
- ❖ Password protect your computer and accounts – remember or secure PINs
- ❖ **Keep you account information up to date & check your credit report at least once a year!!**



Protect your Computer

- ❖ Install and update current virus, firewall, spyware detection and spam blocker software
- ❖ Use a secure browser
- ❖ Do not download or open attachments or links that are suspicious
- ❖ Think twice before using P2P software
- ❖ Use strong passwords
- ❖ Avoid automatic or saved log-ins
- ❖ Securely erase your hard drive before disposing of your computer



Shopping Online

- ❖ Shop only with companies you know
- ❖ Use a secure browser (look for a closed padlock or unbroken key at the bottom of your browser window)
- ❖ Pay only with a credit card or third-party intermediary
- ❖ Track purchases



Impersonations

- ❖ Threaten Arrest / Lawsuit
- ❖ Request immediate payment
 - iTunes gift card
 - MoneyGram
 - Western Union





Sample Case

- ❖ **34 DEFENDANTS CHARGED WITH CONSPIRACY TO COMMIT TAX FRAUD IN BATTLE CREEK**
- ❖ GRAND RAPIDS, MICHIGAN — U.S. Attorney Patrick A. Miles, Jr., announced today that a federal grand jury returned an Indictment charging 34 defendants for their alleged roles in a conspiracy to defraud the IRS through the filing of false tax forms, mostly through using other people’s identification information.
- ❖ The Indictment alleges that the defendants utilized other individuals’ personal identification information (PII)—obtained in part from patients and employees of the Battle Creek Veterans Affairs Medical Center and from inmates of the Michigan Department of Corrections—to file false tax returns. In total, the Indictment alleges that for tax years 2007 through 2014, the co-conspirators, led by lead defendant DERRICK J. GIBSON, filed at least 4,668 federal income tax returns claiming false, fictitious, and fraudulent refunds totaling over \$22 Million.



Resources

- ❖ <https://www.irs.gov/individuals/identity-protection>
- ❖ <https://www.identitytheft.gov/>
- ❖ <http://www.experian.com/>
- ❖ <https://www.transunion.com/>
- ❖ <http://www.equifax.com/>

- ❖ https://www.treasury.gov/tigta/contact_report_scam.shtml



QUESTIONS



CI Contact Info



Internal Revenue Service
United States Department of the Treasury

Richard Ptak, Supervisory Special Agent

616-365-4558

Richard.Ptak@ci.irs.gov

Kim VanderWulp, Special Agent

616-365-4553

Kimberly.VanderWulp@ci.irs.gov