Tax Identity Theft

Presented by
David M. Smith
Special Investigator
Delaware Division of Revenue

Overview

- What is identity theft?
- What is tax identity theft?
- How does tax identity theft happen?
- How does DE Division of Revenue detect identity theft?
- How to lessen your chance of being a victim
- What to do if you're a victim

What Is Identity Theft?

What Is Identity Theft?

- Identity theft is a crime in which someone wrongfully obtains and uses another person's personal information in some way that involves fraud or deception:
  - For example, to fraudulently obtain
    - goods or services
    - a job
    - medical treatment, medications, or equipment
    - government services or benefits
  - hide from government, law enforcement, or others who perform background checks

Fastest Growing Crime in the U.S.

- **Officials warn 500 million financial records hacked**

Erin Kelly, USA Today, October 20, 2014

WASHINGTON – Federal officials warned companies that hackers have stolen more than 500 million financial records over the past 12 months, essentially breaking into banks without ever entering a building.

We're in a day when a person can commit about 15,000 bank robberies sitting in their basement," said Robert Anderson, executive assistant director of the FBI's Criminal Cyber Response and Services Branch.

Fastest Growing Crime in the U.S.

- **Officials warn 500 million financial records hacked (cont.)**

The U.S. financial sector is one of the most targeted in the world, FBI and Secret Service officials told business leaders at a cybersecurity event. The event came in the wake of mass hacking attacks against Target, Home Depot, JPMorgan Chase and other financial institutions.

Nearly 439 million records were stolen in the past six months, said Supervisory Special Agent Jason Truppi of the FBI. Nearly 519 million records were stolen in the past 12 months, he said.

Fastest Growing Crime in the U.S.

- **Officials warn 500 million financial records hacked (cont.)**

About 35% of the thefts were from website breaches, 22% were from cyberespionage, 14% occurred at the point of sale when someone bought something at a retail store, and 9% came when someone swiped a credit or debit card, the FBI said.

About 110 million Americans - equivalent to about 50% of U.S. adults - have had their personal data exposed in some form in the past year, said Tim Pawlenty, president of the Financial Services Roundtable and the former governor of Minnesota.

Recent High-Profile Case

- **JPMorgan Chase Hacking Affects 76 Million Households**

By Jessica Silver-Greenberg, Matthew Goldstein and Nicole Perlroth

October 2, 2014

A cyber-attack this summer on JPMorgan Chase compromised the accounts of 76 million households and seven million small businesses, a tally that dwarfs previous estimates by the bank and puts the intrusion among the largest ever.

Recent High-Profile Case

- **JPMorgan Chase Hacking Affects 76 Million Households**

The details of the breach – disclosed in a securities filing on Thursday – emerge at a time when consumer confidence in the digital operation of corporate America has already been shaken. Target, Home Depot, and a number of other retailers have sustained major data breaches. Last year, the information of 40 million cardholders and 70 million others were compromised at Target, while an attack at Home Depot in September affected 56 million cards.

But unlike retailers, JPMorgan, as the largest bank in the nation, has financial information in its computer systems that goes beyond customers' credit card details and potentially includes more sensitive data.

South Carolina Data Breach

- **South Carolina Tax Department**

In a press conference on November 20th, 2012, Governor Nikki Haley released a report on a cyber-attack on South Carolina's tax collection agency. A spokesman said the hacker tricked a user inside the South Carolina Revenue Department into opening a file that contained a virus and allowed the hacker to access the system.

The Governor released the following figures on the number of people impacted:

Filers impacted: 3.9 million
Dependents: 1.9 million
Businesses: 699,900
Bank Accounts: 3.3 million, some of which are closed

Tax Preparation Office Breaches

- Burglaries of tax preparation offices
- Theft of computers, servers, and client files
- Tax data and personal information of clients being used for refund fraud

Tax Preparers Accused of ID Theft

- **Tax Preparers accused of ID theft, filing false returns**

October 28, 2014

Two tax preparers who operated several tax preparation businesses in the State of Alabama are accused of stealing identities and using them to file more than 900 federal income tax returns totaling more than $2.5 million in refunds.

Although you as a tax preparer may not be involved, you have a significant amount of data that an employee could compromise.

Examples of Information Valuable to Identity Thieves

- Name, address, telephone number
- Date of birth
- Social Security number
- Financial account numbers (bank account or credit card numbers)
- Medicare card number and health insurance number
- Passport number, driver's license number
- Passwords (mother's maiden name, father's middle name)
- Biometric data (fingerprint, iris scan)

How Does Identity Theft Hurt Victims?

- Damage to credit score (and reputation)
- Hurt your Job Prospects (Employment ID Theft)
- Cause your Auto Insurance Rates to Rise
- Get you a Surprise Tax Bill or Delay your Refund (Tax ID Theft)
- Get you the Wrong Treatment at a Hospital (Medical ID Theft)
- Prevent your Kids from Getting College Financial Aid (Child ID Theft)
- Possible civil judgments or criminal record (Criminal ID Theft)
- Kill You (Virtually) - database shows you as deceased

What Is Tax Identity Theft?

What Is Tax Identity Theft?

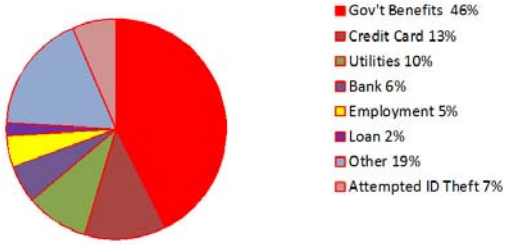
- Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job.
  - Filing a fraudulent tax return using another person's Social Security number
  - Claiming someone else's children as dependents
  - Claiming a tax refund using a deceased taxpayer's information
  - Earning wages under another person's Social Security number

Scope of the Problem

Delaware DOR Statistics:

- 2011: 500 incidents of identity theft
  - **$416k refunds claimed** / $19k issued
  - 95% of fraudulent refunds stopped
- 2012: 1,378 incidents of identity theft
  - **$1,338,000 refunds claimed** / $20k issued
  - 98% of fraudulent refunds stopped
- 2013: 2,017 incidents of identity theft
  - **$2,930,000 refunds claimed** / $81k issued
  - 97% of fraudulent refunds stopped

How Victims' Information is Misused



Source: FTC Consumer Sentinel Data Book 2012

Types of Government Benefits Fraud

- Tax or wage-related fraud 43.4%
- Gov't benefits applied for/received 1.6%
- Other gov't docs issued/forged 0.8%
- Driver's license issued/forged 0.6%

- TOTAL: 46.4%

Source: FTC Consumer Sentinel Data Book 2012

Top 10 States for Tax Identity Theft

Florida
Georgia
California
Michigan
New York
Nevada
Texas
Arizona
Maryland
Alabama

Source: FTC Consumer Sentinel Data Book 2012

How Does Tax Identity Theft Happen?

How Does Tax Identity Theft Happen?

- Tax identity theft is often perpetrated by large criminal groups with individuals at all stages of the scheme.
  - Those who steal Social Security Numbers (SSNs) and personal identifying information
  - Those who file false returns with the government
  - Those who facilitate obtaining the refunds through electronic payments
  - Ringleaders who promote the schemes
- Tax identity theft often crosses state borders, and increasingly national borders.

11 Ways to Become a Victim of Tax Identity Theft

(through no fault of your own)

1. **Get Medical Care**

A Florida man admitted in a November 2012 guilty plea that while working as a financial services representative for a local health care provider in FL, he sold tax refund fraudsters 400 patient IDs. He also acknowledged using patient IDs to file multiple fraudulent tax returns himself using TurboTax.

11 Ways to Become a Victim of Tax Identity Theft

(through no fault of your own)

2. **File a Tax Return on Paper**

A California woman who worked as a part-time data entry clerk at an IRS office, stole 68 paper tax returns whose data hadn't been entered into IRS computers, and used the information to file electronic fraudulent tax returns claiming more than $1.7 million in fraudulent refunds.

11 Ways to Become a Victim of Tax Identity Theft

(through no fault of your own)

3. Serve your Country

In December 2012, a Miami man was sentenced to 57 months in federal prison after admitting that while stationed as a Marine in Afghanistan, he emailed the names, birth dates and Social Security numbers of more than 100 of his fellow marines to a co-conspirator in Florida who submitted fraudulent 2011 refund claims. In return for providing the personal information, the ex-marine was to get 50% of any refunds issued. Military personnel serving in combat zones don't have to file their tax returns until 180 days after leaving the zone, which makes them tempting targets for identity thieves who can file fraudulent returns with little concern that the real taxpayer will file first.

11 Ways to Become a Victim of Tax Identity Theft

(through no fault of your own)

4. Use a Dishonest Tax Preparer

A former Ga. tax return preparer was sentenced in January 2013 to five years in prison after pleading guilty to filing false tax returns in the names of deceased individuals, and using the IDs of former clients of his tax preparation business he had run out of his home.

11 Ways to Become a Victim of Tax Identity Theft

(through no fault of your own)

5. Use an Honest Tax Preparer

In October 2012, a North Carolina man was sentenced to 125 months in prison for breaking into a Jackson Hewitt office and stealing the files of more than 300 tax clients, then using the information to file fraudulent tax returns and claims for refund. The refunds were directed to either debit cards which were mailed to addresses which he knew were vacant, or to bank accounts that were opened, using fraudulent and unauthorized information.

11 Ways to Become a Victim of Tax Identity Theft
(through no fault of your own)

6. Have an Unsuspecting Employer

A New York resident pled guilty in July 2012 to a tax identity theft scheme charging, among other things, that he got personal information from some employers by posing as an IRS employee claiming to be an "Audit Group Representative," demanding the names, Social Security numbers and birth dates of their workers. On one occasion, according to the indictment, he told the employer he was involved in preventing identity theft.

11 Ways to Become a Victim of Tax Identity Theft
(through no fault of your own)

7. Get Behind on your Bills

In December 2012, an Alabama federal grand jury charged a woman with stealing debtor IDs from the collection agency where she worked and giving the information to her son-in-law, who along with a second man, allegedly used it to file fraudulent 2011 tax returns.

11 Ways to Become a Victim of Tax Identity Theft
(through no fault of your own)

8. Have Internet Installed at your Home

In May 2013, an Alabama man who worked as an Internet service installer was sentenced to 30 months in prison for using the IP addresses of his customers to file 27 fraudulent tax returns requesting more than $90,000 in refunds so as to make it seem that the customers themselves were filing those returns. The man also owned and operated a tax return business in Alabama.

11 Ways to Become a Victim of Tax Identity Theft

(through no fault of your own)

9. Get Sentenced to Prison

In July 2012, a Florida woman was sentenced to 25 months for stealing prisoner identities while she worked as a correctional officer at a state facility in Florida and then giving the data to a crooked tax preparer who filed fraudulent refund claims for more than $1.3 million in the names of 120 inmates. In January 2013, a Virginia man pleaded guilty to filing at least 25 phony tax returns using the identities of his fellow inmates in federal prison --- without their permission.

11 Ways to Become a Victim of Tax Identity Theft

(through no fault of your own)

10. Take out a Student Loan

An Alabama woman is serving a 94 month sentence after a jury convicted her of 13 counts, including identity theft and conspiracy to commit tax fraud. Prosecutors said that while a customer service rep for student loan processor EDS, she stole the names and social security numbers of 54 student loan borrowers and gave them to a crooked tax preparer.

11 Ways to Become a Victim of Tax Identity Theft

(through no fault of your own)

11. Be down on your Luck

In December 2012, a California woman admitted that while a receptionist for the L.A. County Department of Public Social Services, she logged into a computer database of public assistance applicants and recipients and took screen shots of the personal ID information of at least 132 of them. The IDs of 64 of them were used by her husband and others to file false 2011 refund claims that caused $358,000 in losses to the IRS.

"Queen of IRS Tax Fraud"

- Rashia Wilson from Tampa helped publicize the issue of tax identity theft, in part because of the colorful way in which she boasted about her activities.
- Posted on her Facebook page that she was the "Queen of IRS tax fraud" along with a picture that showed her holding stacks of cash.
- Dared the government to catch her, writing on her Facebook page, "I'm a millionaire for the record, so if U think indicting me will B easy it won't, I promise you!"
- Indicted in December 2012 and sentenced last year to 21 years in jail
- Bought a 2013 Audi with a cashier's check for $92,682.67

How Does Tax Identity Theft Happen?

- Identity thieves continue to adjust tactics and play on volume
- Submit large numbers of false returns electronically in the hopes that some of them will get through IRS and DOR filters.
- Rather than steal identities wallet by wallet, they steal names and social security numbers by the dozens, or the hundreds, or the thousands.
- Often with the help of corrupt insiders with access to personal data, including tax preparers, health care staff, government employees, debt collectors, etc.

How Does Tax Identity Theft Happen?

- Theft by employees, family, friends, visitors, advisors
- Your trash, Your wallet, Your computer, Your mail
- Buying information from corrupt insiders or volunteers at:
  - **check cashing businesses**, banks, debt collectors
  - **nursing homes**, hospitals, clinics, medical offices
  - prisons
  - schools, government offices
  - tax preparation offices
- The easiest way for an identity thief to get information is to just "Ask For It" (unsolicited calls from telemarketers, phishing e-mails, etc.) – tends to be the exception

How Does Tax Identity Theft Happen Online?

- Data breaches, hacking into computers and networks
- Phony emails from imposters
- Unsecure Wi-Fi hotspots
- Peer-to-peer file sharing
- Social networking
- Downloading software or apps from unknown sources

Simplistic Example of Tax Identity Theft

- 650 tax returns were all transmitted from a single IP address at the home of an Alabama woman
- More than 400 of these returns claimed a tax refund of exactly $1,300
- Every tax return claimed the taxpayer received wages from, and had taxes withheld by WalMart
- Received more than $1.2 million paid on WalMart MoneyCards and other pre-paid debit cards

Common Sources of Identity Theft

- Death Master File
- Schools
- Prisons
- Medical offices
- Nursing Homes
- Copy Machines (hard drives)
- Phony apartment & job listings on Craigslist
- Government Offices
- Financial Institutions
- Tax Preparers
- Volunteer Associations

Warnings Signs of Possible Tax Identity Theft

- Social Security number is lost, stolen, or compromised
- Unusual delay in getting a refund
- IRS notification:
  - duplicate tax return filing
  - unreported income
  - duplicate dependents

How Does Delaware Detect Identity Theft?

How Does Delaware Detect Tax Identity Theft

- Delaware Division of Revenue uses Identity Theft filters to detect and reduce identity theft
- These filters are increasingly successful in flagging suspicious returns and preventing the issuance of fraudulent refunds
- Pattern matching and trends used to identify fraud
- Timely access to third-party income and withholding information at the time tax returns are processed is the most important tool

Identity Theft Filters

- Division of Revenue continues to expand the number of identity theft filters it uses to identify potentially fraudulent tax returns
- The identity theft filters incorporate criteria based on characteristics of confirmed identity-theft tax returns
- Tax returns identified by these filters are held during processing until DOR can verify the taxpayer's identity

Identity Theft Filters

- Identity Theft filters consist of the following:
  - Limiting multiple refunds to a single bank account (indication of fraudulent activity)
  - Comparing first-time filer information to Unemployment data
  - Detecting duplicate returns
  - Placing Identity Theft indicators on accounts

Characteristics of Fraudulent Tax Returns

- Typically filed electronically and early in the tax filing season
- Common characteristic is the reporting of false income and withholding to generate a fraudulent tax refund
- The majority of tax returns identified as identity theft returns involved the use of a pre-paid debit card
- High withholding tax ratio
- Suspicious employers (EINs)
- Duplicate bank accounts
- Suspicious Preparer IDs (PTINs)
- Duplicate Telephone #s / E-mail Addresses

Goals of Identity Theft Filters

- Increase DORs ability to identify and reduce fraud
- Reduce total amount of improper payments
- Expedite the processing of compliant returns
- Assist taxpayers who may fall victim to fraud with a single point of contact

Trends in Tax-Related Identity Theft

- Deceased individuals (Death Master File)
- Identities of Puerto Rican citizens
- Prisoner returns
- Military personnel
- Medical professionals
- Individuals not required to file returns
- Anticipate children's SSNs (dependents)
- Anticipate reusing victim's SSNs

How To Lessen Your Chance of Being a Victim

Reducing the Risk of Tax Identity Theft

- Minimize personal information in purses or wallets, or on smartphones
- Shred financial documents before disposing
- Don't give out personal information unless you know who's asking for it and why they need it
- Keep personal information secure — at home, at the office, in your car
- Don't click on links sent in unsolicited email

Reducing the Risk (cont.)

- Monitor accounts and review financial statements regularly
- Watch mail for credit card statements or accounts that you didn't open
- Confirm you get the statements you expect in the mail
- Get your free annual credit report at www.annualcreditreport.com
- Make a copy of everything in your wallet and store it safely

Preparing and Filing Tax Returns

- Know your tax preparer
- Mail tax returns as early in the tax season as possible
- Mail tax returns directly from post office
- If filing electronically, use a secure network and encrypt
- Store copies of your returns in a secure place
- Shred drafts, calculation sheets, and extra copies
- Do not respond to unsolicited emails that appear to be from the IRS or the Division of Revenue

Additional Advice for Older Americans

- Protect Medicare card number, which might be SSN
- Protect personal information at home like you would cash or jewelry
- Make sure to open and review your mail and email
- Ask medical and care facilities about their data protection policies
- Select assistants and other support professionals with care

What to Do If You're a Victim

Steps for Tax Identity Theft Victims

- Contact the IRS Identity Protection Specialized Unit at 800-908-4490
- Contact DOR - David M. Smith at 302-577-8958
- File IRS Identity Theft Affidavit (Form 14039)
- Have valid identification (government-issued identification: Social Security card, driver's license, or passport)

Steps for Tax Identity Theft Victims

- Contact credit reporting agencies
  - place a fraud alert
  - consider a credit freeze
  - request and review your credit report
- File a report with local police agency
- Contact Delaware Attorney General's Office
  - (800) 220-5424
  - Obtain Identity Theft Passport
- Go to: irs.gov/identitytheft

Fraud Alerts

- Expires in 90 days
- Renewable for 7 years
- Entitles victim to one free credit report
- Need to call only one of the three credit reporting agencies; it will notify the others:
  - Equifax: 800-525-6285
  - Experian: 888-397-3742
  - TransUnion: 800-680-7289
- Creditors **must** contact you prior to making any changes to your existing accounts, and/or opening any new accounts

Credit Freezes

- Tool that allows you to restrict access to your credit report
- Must request in writing from each credit reporting agency
- Blocks all new credit without your authorization, but won't stop a thief from making charges to existing accounts
- Effective until lifted

Resources

ftc.gov/idtheft
for the FTC's Identity Theft Resources

ftc.gov/taxidtheft
for Tax Identity Theft Awareness Week

Resources

FTC: ftc.gov/idtheft
ftc.gov/taxidtheft

IRS: irs.gov/identitytheft

Dept. of Justice - Office for Victims of Crime (OVC): ovc.gov

National Identity Theft Victims' Assistance Coalition (NITVAN): identitytheftnetwork.org

Identity Theft Resource Center (ITRC): idtheftcenter.org

David M. Smith
Special Investigator
Delaware Division of Revenue
david.m.smith@state.de.us
302-577-8958