

Personal and School District Income Tax Refund Fraud

Pat Zimmerman and David Peck

Personal & School District Income Tax Division



Department of
Taxation

Stolen Identity Refund Fraud

SIRF- quick facts



- Identity Theft is the fastest growing crime with 9.9 million incidents per year (according to the FTC)
- Per the IRS, in 2014 over 2.7 million taxpayers had their ID's compromised
- Through the end of September 2016:
 - Per the IRS, they identified 787k returns for \$4B fraudulent refund claims compared to 1.2M returns for \$7.2B in first 9 months of 2015.
 - 50% less IRS ID theft affidavits from last year (275k)
 - ~74k returns claiming \$372M were flagged and not paid due to reports generated by tax industry partners

Where is the data coming from?

- Data breaches



Identity Theft Resource Center 2016 Data Breach Category Summary



How is this report produced? What are the rules? See last page of report for details.

Report Date: 10/19/2016

Totals for Category: Banking/Credit/Financial	# of Breaches: 33 % of Breaches: 4.2%	# of Records: 26,262 %of Records: 0.1%
Totals for Category: Business	# of Breaches: 338 % of Breaches: 43.2%	# of Records: 2,541,158 %of Records: 8.6%
Totals for Category: Educational	# of Breaches: 71 % of Breaches: 9.1%	# of Records: 488,514 %of Records: 1.7%
Totals for Category: Government/Military	# of Breaches: 55 % of Breaches: 7.0%	# of Records: 12,290,322 %of Records: 41.6%
Totals for Category: Medical/Healthcare	# of Breaches: 286 % of Breaches: 36.5%	# of Records: 14,189,398 %of Records: 48.0%
Totals for All Categories:	# of Breaches: 783 % of Breaches: 100.0	# of Records: 29,535,654 %of Records: 100.0%

2016 Breaches Identified by the ITRC as of: 10/19/2016

Total Breaches: 783
Records Exposed: 29,535,654

Top 10 data breaches 2016

- Department of Fish and Wildlife (ID, KY, OR, WA) ~5.76 million
- US Office of Child Support Enforcement (WA) ~5 million
- Banner Health (AZ) ~3.7 million
- Newkirk Products (NY) ~3.3 million
- 21st Century Oncology (FL) ~2.2 million
- Verizon (NJ) ~1.5 million
- Centene (MO) ~950k
- Valley Anesthesiology & Pain Consultants (AZ) ~882k
- Bon Secours Health Systems/R-C Healthcare Mgmt (MD) ~655k
- Kroger/Equifax W-2 Express (GA) ~431k



Where is the data coming from? (cont'd)

- Phishing schemes
 - Business E-mail compromise (BEC)
 - Authentic looking e-mail sent to payroll/HR from high ranking executive/CEO requesting W-2 info



Where is the data coming from? (cont'd)

- Employer BEC Phishing Breach letter example (pg 1)

March 21, 2016

Dear Barb:

LLC is committed to protecting the security and confidentiality of the personal information we maintain related to our employees and former employees. Regrettably, we are writing to inform you of an incident involving some of that information.

On March 15, 2016, we learned that W-2 tax forms related to some of our current and former salaried employees had been emailed to an unauthorized individual as a result of a phishing email. The information was sent under the belief that the phishing email was a legitimate, internal company request. Upon learning this, we immediately contacted federal law enforcement and are working with them to investigate the incident. The emailed W-2 forms contained your name, address, Social Security number, and income information.

Where is the data coming from? (cont'd)

- Employer BEC Phishing Breach letter example (pg 2)

We have already notified the IRS on your behalf; so that they can monitor for suspicious activity. Additionally, to help you detect possible misuse of your information, we are offering you a complimentary one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you and enrolling in this program will not hurt your credit score. Unfortunately, due to privacy laws, we are not able to enroll you directly. **For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, as well as information from the IRS on tax-related identity theft, please see the additional information provided in this letter.**

We deeply regret any inconvenience this may have caused you. To help prevent something like this from happening in the future, we are re-educating our employees regarding phishing emails and reviewing our internal procedures related to requests for sensitive information. If you have any questions, please call

Sincerely,

EXAMPLE

Director of Safety and Human Resources

Where is the data coming from? (cont'd)

- Over 125 known BEC phishing breaches reported to Ohio since mid March 2016
 - Examples:
 - Milwaukee Bucks NBA basketball team
 - Sprouts Farmer's Market
 - Universities/community colleges
- Sharing with the IRS and other states is vital

Where is the data coming from? (cont'd)

- Preparer breaches
 - Fraudster hacks into prep software and submits unfiled returns
 - Ransomware
 - Demands bitcoins/online currency in exchange for giving client data back
 - Both schemes occurred to Ohio based preps in 2016



Data sold on dark web

- TOR (www.torproject.org)
 - US Naval research
 - Donated computer servers
 - Data encrypted through random pathways/nodes
- Silk Road
- Alpha Bay Market
 - ~20k fraud items for sale
- “Fullz” are often sold on per ID basis for bitcoin/online currencies

Dark web example 1

Make a killing with tax refunds!!! (#1 (permalink))

 **meyarobert** is Online
VIP member

Rep Power: 0


Posts: 124
Thanks: 26
Thanked 320 Times in 22 Posts
Join Date: Jul 2014
Location: 127.0.0.1
Age: 20

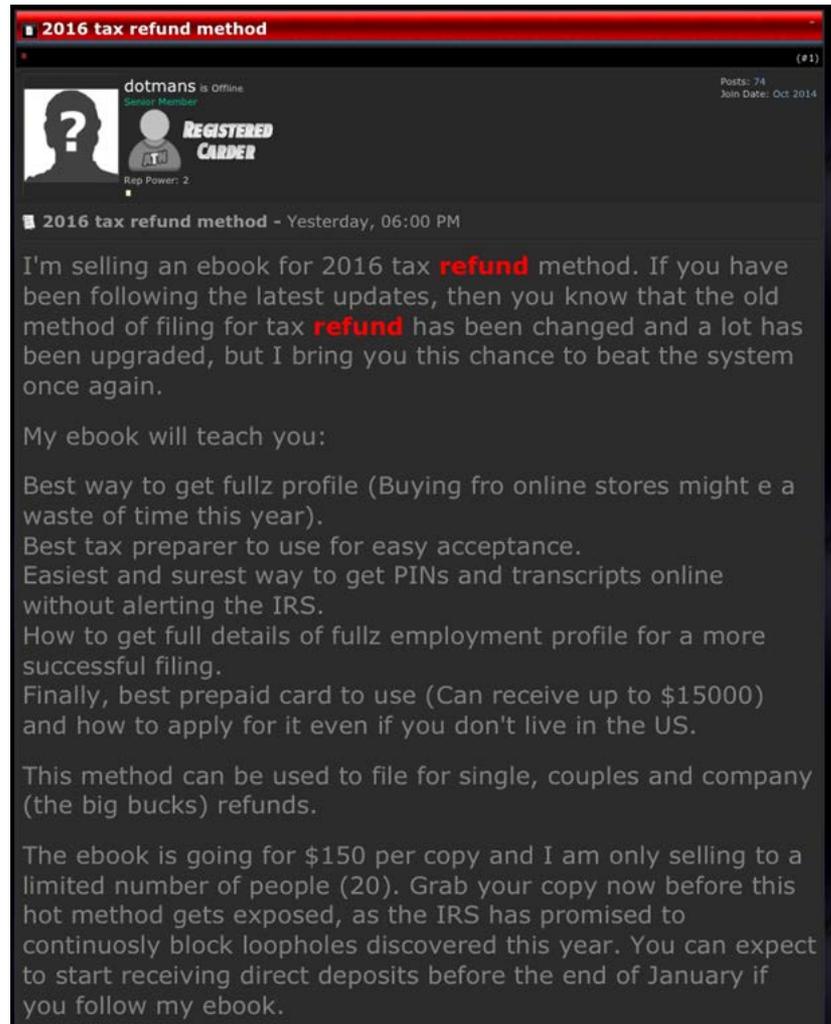
 **Make a killing with tax refunds!!!** - Yesterday, 11:56 PM

Tax Refund for 2016
100% success rate proofs below
From 3000(single) usd
7000usd and above (married filling jointly) for federal
2000(single)usd state
11000usd and above(married filling jointly) for state

Filling into prepaid cards and us accounts excluding chase bank and wells fargo.

prices for filing:
200 usd for single with (w2 or transcript)
250 usd for single with fulls
300 usd for single without fulls(or w2 or transcript)

Dark web example 2



The screenshot shows a forum post in a dark-themed browser window. The window title is "2016 tax refund method". The post is by a user named "dotmans", who is offline and has a reputation power of 2. The user's profile picture is a silhouette with a question mark, and they have a "REGISTERED CARDER" badge. The post content is as follows:

2016 tax refund method - Yesterday, 06:00 PM

I'm selling an ebook for 2016 tax **refund** method. If you have been following the latest updates, then you know that the old method of filing for tax **refund** has been changed and a lot has been upgraded, but I bring you this chance to beat the system once again.

My ebook will teach you:

- Best way to get fullz profile (Buying fro online stores might e a waste of time this year).
- Best tax preparer to use for easy acceptance.
- Easiest and surest way to get PINs and transcripts online without alerting the IRS.
- How to get full details of fullz employment profile for a more successful filing.
- Finally, best prepaid card to use (Can receive up to \$15000) and how to apply for it even if you don't live in the US.

This method can be used to file for single, couples and company (the big bucks) refunds.

The ebook is going for \$150 per copy and I am only selling to a limited number of people (20). Grab your copy now before this hot method gets exposed, as the IRS has promised to continuously block loopholes discovered this year. You can expect to start receiving direct deposits before the end of January if you follow my ebook.

Dark web example 3

The image shows a screenshot of a web browser displaying the IRS.gov "Refund Status Results" page. A large, semi-transparent green watermark with the alphanumeric string "N3140d" is overlaid on the left side of the page. The browser's address bar shows the URL "https://sa.www4.irs.gov/irfof/lang/en/irfofresults.jsp" and the search ID "n3790d". The page content includes the IRS logo, navigation tabs for "Home", "Get Refund Status", "Refund Information", "Take Survey", and "Log Out". The main heading is "Refund Status Results". A progress bar indicates the status: "Return Received" (orange), "Refund Approved" (orange), and "Refund Sent" (light orange). A message box states: "Your return has been processed and refund amount approved." Below this, it says: "Your tax refund is scheduled to be sent to your bank by February 1, 2016." A "Please Note" section advises: "For refund information, please continue to check here, or use our free mobile app, IRS2Go. Updates to refund status are made no more than once a day." The page also includes a link to the "IRS Privacy Policy". The Windows taskbar at the bottom shows the time as 3:51 PM on 2/1/2016.

Refund Status Results

https://sa.www4.irs.gov/irfof/lang/en/irfofresults.jsp

n3790d

Most Visited Getting Started Bank Accounts - Open... Free File Fillable Forms

IRS.gov

Home Get Refund Status Refund Information Take Survey Log Out

Your Personal Tax Refund Status Results

Return Received Refund Approved Refund Sent

Your return has been processed and refund amount approved.

Your tax refund is scheduled to be sent to your bank by **February 1, 2016**.

If your refund is not credited to your account by **February 5, 2016**, check with your bank to see if it has been received.

Please Note:
For refund information, please continue to check here, or use our free mobile app, IRS2Go. Updates to refund status are made no more than once a day.

[IRS Privacy Policy](#)

EN 3:51 PM 2/1/2016

Where is the data coming from? (cont'd)

- Account Takeovers (ATO)
- IRS Get Transcripts
- Older hacks data
 - OPM
 - TurboTax
 - Sony
 - Chase
 - Anthem



Combating Fraud- ID Quiz

Utilizing ID Confirmation Quiz

- 60 % reduction in quiz letters from CY 2015.
- We anticipate further reductions in the coming years.



*Personal Income Tax
Manual Review Unit
P.O. Box 182847
Columbus, OH 43218
Telephone: 1-855-855-7579
Fax: 206-339-3285
TTY/TDD: 1-800-750-0750*

IDENTITY CONFIRMATION QUIZ: OHIO'S COMMITMENT TO STOPPING TAX FRAUD

February 7, 2016

TAXPAYER, JOE
123 MAIN ST
COLUMBUS OH

43229

Reference Number: 1234567
Authorization Code: 1234567890

RE: 2015 Ohio Personal Income Tax Return

SSN/ITIN: XXX-XX-1234

Dear Taxpayer,

ID Quiz Tutorial and FAQ's

- ID Quiz Tutorial and FAQ's available on ODT's website to assist TP's and preps

For more details regarding the quiz, watch the tutorial below:

If you have trouble viewing the video on this page, [click here](#) to view the video directly on YouTube.



To begin the quiz or identify the return as suspicious click the **blue** button below.

Take Quiz/Identify Return as Suspicious

Combating Fraud– (cont'd)

Implemented Analytics model in late CY 2015

- Provided ability to reduce false positives
 - Efforts in this area continue



Combating Fraud– Self reporting fraud



ID Quiz: Log In

Answer Questions

View Results

If you received a letter from the Ohio Department of Taxation directing you to this web site, we need to confirm some information before the processing of your tax return can continue.

Before starting this process, please have ALL the information available referenced in the letter you received.

- I filed a tax return / I had a tax return filed on my behalf. I wish to take the Ohio Identity Verification Quiz so my return can continue processing.
- I **DID NOT** file a tax return / I **DID NOT** authorize to have a tax return filed on my behalf. I wish to report that return as suspicious.

Please enter the following information to report this tax return as suspicious and have it examined by an agent.

Reference Number: (from letter)

Authorization Code: (from letter)

Continue

Self-Reporting Fraud

 I ***DID NOT*** file a tax return / I ***DID NOT*** authorize to have a tax return filed on my behalf. I wish to report that return as suspicious.

- 1,340 returns for \$4.2M reported by taxpayers
- 134 false positives marked in error by taxpayer representing \$88,221

Fraud Trends

2014

- ODT Income Tax fraud hit an all time high for suspect refunds amounts requested.

2015

- ODT saw an increase in refund attempts but a reduction in refund amounts.

2016

- ODT saw a reduction in both refund attempts and refund amounts.



Criminal Investigation items

- Known preparer schemes
 - Improved efforts in this area continue
- Ohio based
 - Youngstown individual (October 2015)
 - 1 year in prison
 - 3 years supervised release
 - Restitution owed
 - Toledo individual (August 2015)
 - 8 years of supervised release
 - Restitution owed
 - Community service & Drug/Alcohol program
- Non-Ohio based
 - Four Miami, Florida individuals (June 2015)
 - 4 years in prison
 - 3 years supervised release
 - Restitution owed
 - One Miami, FL individual (March 2016)
 - 7 years in prison
 - 3 years supervised release
 - Restitution owed



Preps- Pass through banks

- Commons banks fraudsters are using as “middle-man” accounts as a forensic countermeasure
 - Guaranteed payment to preps/software companies from tax refund
 - Examples:
 - Ohio Valley Bank (Ohio)
 - Republic Bank (Kentucky)
 - First Century Bank (Georgia)
 - River City Bank (Kentucky)



Preps- Protecting your clients & yourself

- Legal responsibility of businesses & individuals that maintain, share, transmit or store taxpayer data to have safeguards in place to protect client information.
- Review **IRS Publication 4557**
 - The need to safeguard taxpayer data
 - Security (facilities, personnel, IT, computer systems, media)
 - Reporting incidents
 - Laws & regulations
 - Best practices



Preps- Network protection

- Protecting your network is critical
 - Set up strong required passwords to access, modify, or transmit returns when connected to the network (**remote access**)
 - Make sure all firewalls and anti-virus software are up to date
 - Be cognizant of phishing e-mails (clicking on attachments or links)
 - Encrypt e-mails with taxpayer data
 - Periodic training with new/existing employees especially those with remote access to your network



Preps- Monitor client returns

1. Carefully monitor which returns have or haven't been filed yet with your PTIN
2. Be cognizant of unexpected acknowledgements, etc.
3. Be aware of rejected returns for returns already on file
 - If you receive any of the above:
 - Communicating w/IRS & states is vital

<https://www.irs.gov/uac/irs-security-awareness-tax-tips>



Preps- Some steps resolve a breach

- Hire IT resources to provide assistance in protecting your system going forward
- Contact local law enforcement/FBI
- Contact the IRS/state taxing agencies affected
 - Being assigned a new EFIN/PTIN
 - Making agencies aware for fraud detection
- Notify clients of breach
- Assist clients to get legit returns processed as timely as possible

Preps- How to assist tax ID theft victims?

- SPIKES method

Setting

Perceptions

Invitation

Knowledge

Emotions

Strategy



Preps- How to assist tax ID theft victims?

- Advise the taxpayer who they should contact immediately to alert of the ID theft committed:
 - IRS & States
 - Local law enforcement
 - FTC
 - BMV
 - Credit bureaus
- Assist the taxpayer in submitting their paper income tax return with all wage statements
 - Assist the taxpayer in submitting their ID theft affidavit(s)
- Help the taxpayer with any follow-up on their ID theft situation and manage their expectations



Preps- How to assist tax ID theft victims? (cont'd)

- Ohio specific paper ID theft affidavit available on ODT website
- ODT will accept IRS 14039 as well



**Department of
Taxation**

Tax Technical/ID Theft Research
P.O. Box 182847
Columbus, OH 43218-2847
Phone: (800) 282-1780
eFax: (253) 234-1371



13240106

IT TA
Rev. 7/16

Identity Theft Affidavit

Full legal name
First name M.I. Last name

Address

City State ZIP

Social Security number
(only the last four digits are required)

Daytime phone
(enter only numbers, no dashes or parentheses)

E-mail address

You are required to attach a photocopy of your current driver's license or state issued identification card.

What tax year(s) are you claiming your identity was stolen?

Preps- How to assist tax ID theft victims? (cont'd)

- Visit ODT's website (tax.ohio.gov)- Individual/Identity Theft tab; FAQ's- Income- Identity Theft

Income - Identity Theft	▼
Expand All	
1. What is identity theft?	
2. What are the warning signs of income tax related identity theft?	
3. Tax identity theft victims-victims with an Ohio income tax filing requirement.	
4. Tax identity theft victims-victims without an Ohio income tax filing requirement	
5. Tax identity theft victims-recommended for all victims.	
6. Tax preparers with clients who are income tax identity theft victims.	
7. How do thieves typically obtain access to personally identifiable information (PII)?	
8. What are some tips to safeguard your SSN and other personal information?	
9. How to protect your child from identity theft?	
10. What are some additional identity theft resources?	
11. I received an Ohio identity confirmation quiz letter, but I DID NOT file an income tax return with the state of Ohio. What should I do?	
12. If I had to confirm my identity with the Ohio Department of Taxation in filing my 2014 Ohio IT-1040, will I have to confirm my identity again this year when filing my 2015 Ohio IT-1040?	
13. What does the Ohio Department of Taxation do to pursue perpetrators of ID Theft returns?	
14. Do you have a tax related identity theft question we did not answer?	

Taxation Resources

- Download ODT's Mobile app
 - Refund Status
 - Facebook
 - Contact Us
 - Sales Tax Rate Finder

- Sign up for Tax Alerts on ODT's homepage



Tax
Alerts

Contact Us

- Personal & School District Income Tax
 - 800-282-1780 (General #)
 - 614-728-1055 (Tax Practitioner #)
 - Via e-mail at tax.ohio.gov “Contact Us”
 - Survey for your feedback of how we are doing



Department of
Taxation