

A photograph of the Golden Gate Bridge in San Francisco, viewed through a chain-link fence. The bridge's towers and suspension cables are visible in the background, partially obscured by the diamond-shaped mesh of the fence in the foreground. The sky is a pale, hazy blue.

NCSL Presentation

Saving Treasuries Substantial Revenue through State
DOR, IRS and Private Sector Collaboration

**Julie Magee Director, Tax
Regulatory Affairs**

Background on Credit Karma

- Free credit scores, credit reports, credit monitoring, financial management tools and more
 - Over 75M members
 - Over 1B scores to consumers
 - Over \$500M in revenue
 - Nearly 1M federal tax filings last year, approximately 750,000 state returns
- Helping members make financial progress in the US and parts of Canada
- Offices in San Francisco, Los Angeles, Charlotte, Cary
- Launched Credit Karma Tax January 2017

Agenda

In the past, Federal and State Treasuries allowed criminals to steal billions of dollars through the annual income tax filing obligation but recent innovations by all stakeholders have made it much more difficult to defraud government taxing agencies. Learn how this public private partnership is saving your state millions of dollars every year and better protecting your constituents from identity theft.

- Criminal use of tax products
- State efforts
- Security Summit
- Future State

Criminal Use of Stolen Identities in the Tax World

First - Understand the Threat

- The Department of Revenue is a treasure trove of data that can be converted to stolen income tax refunds, and any other government financial claim that can be obtained in your state.
 - Unemployment compensation
 - Housing
 - Medical expenses
 - They are very creative and BOLD

Tax refund fraud is more financially rewarding than running drugs on the street. Less chance of dying or getting caught and it pays much better!

Scope of Problem - Tax Refund Fraud

GAO Highlights

Highlights of GAO-15-119, a report to congressional requesters

Why GAO Did This Study

IRS estimated it prevented \$24.2 billion in fraudulent identity theft (IDT) refunds in 2013, but paid \$5.8 billion later determined to be fraud. Because of the difficulties in knowing the amount of undetected fraud, the actual amount could differ from these point estimates. IDT refund fraud occurs when an identity thief uses a legitimate taxpayer's identifying information to file a fraudulent tax return and claims a refund.

GAO was asked to review IRS's efforts to combat IDT refund fraud. This report, the second in a series, assesses (1) the quality of IRS's IDT refund fraud cost estimates, and (2) IRS's progress in developing processes to enhance taxpayer authentication.

GAO compared IRS's IDT estimate methodology to GAO Cost Guide best practices (fraud is a cost to taxpayers).

January 2015

IDENTITY THEFT AND TAX FRAUD

Enhanced Authentication Could Combat Refund Fraud, but IRS Lacks an Estimate of Costs, Benefits and Risks

What GAO Found

Identity Theft (IDT) Refund Fraud Cost Estimates. The Internal Revenue Service's (IRS) fraud estimates met several GAO Cost Guide best practices, such as documenting data sources and detailing calculations. However, the estimates do not reflect the uncertainty inherent in measuring IDT refund fraud because they are presented as point estimates. Best practices suggest that agencies assess the effects of assumptions and potential errors on estimates. Officials said they did not assess the estimates' level of uncertainty because of resource constraints and methodological challenges. Because making different assumptions could affect IDT fraud estimates by billions of dollars, a point estimate (as opposed to, for example, a range) could lead to different decisions about allocating IDT resources. Reporting the uncertainty that is already known from IRS analysis (and conducting further analyses when not cost prohibitive) might help IRS communicate IDT refund fraud's inherent complexity.

IRS Estimates of Attempted IDT Refund Fraud, 2013

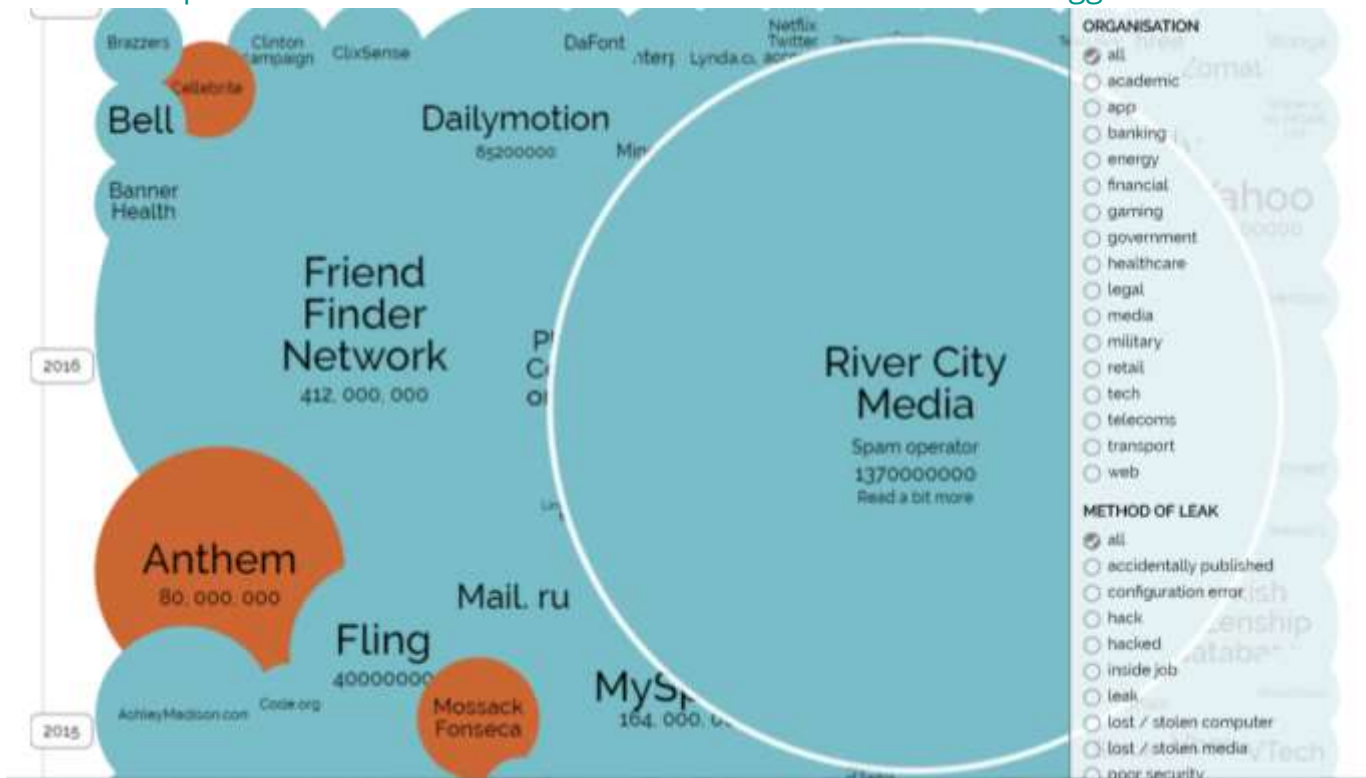


Source: GAO analysis of IRS data. | GAO-15-119

In 2013 the IRS paid out \$5.8 Billion to criminals who filed fraudulent refunds. State returns are linked to the federal return so while not a one to one correlation always, most of the time a state will see the same fraudulent return that the IRS did.

Fueled by the Plethora of Stolen Data Flooding the Dark Web

- <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>



<https://haveibeenpwned.com/>

The screenshot shows the homepage of the website 'Have I Been Pwned'. At the top, there is a dark navigation bar with a logo on the left and several menu items: 'Home', 'Notify me', 'Domain search', 'Who's been pwned', 'API', 'About', and 'Donate' with a Bitcoin icon. The main content area has a blue background. In the center, there is a large white rounded rectangle containing the text '';--have i been pwned?'. Below this, a smaller line of text says 'Check if you have an account that has been compromised in a data breach'. Underneath is a search interface with a white input field containing the placeholder text 'email address or username' and a dark button labeled 'pwned?'. At the bottom, a dark footer contains four statistics: '227 pwned websites', '3,914,073,118 pwned accounts', '52,719 pastes', and '49,836,833 paste accounts'.

Category	Count
pwned websites	227
pwned accounts	3,914,073,118
pastes	52,719
paste accounts	49,836,833

It is highly likely some or all of your info is already out on the dark web.


Oh no — pwned!

Pwned on 4 breached sites and found no pastes (subscribe to search sensitive breaches)


[Notify me when I get pwned](#) [Donate](#)

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

 **Adobe:** In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poor and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

 **Modern Business Solutions:** In October 2016, a large Mongo DB file containing tens of millions of accounts was shared publicly on Twitter (the file has since been removed). The database contained over 58M unique email addresses along with IP addresses, names, home addresses, genders, job titles, dates of birth and phone

W2s For Sale in the Underground Market

BANKS SHOP PAYPAL DEBITCARD OTHER

W-2 2016 (3607)

Name	Age	City	State	Zip	SSN	Gender	DOB	Checked	Refers	Price	Actions
DAK	48K	BOCA RATON	FL	33486	*****	MA	NA	(11-01-1987)	kasahk	155	🛒 / +
ANTONIO	39K	COLRAY BEACH	FL	33444	*****	MA	NA	(11-01-1987)	kasahk	145	🛒 / +
ROBERTO	39K	WEST PALM BCH	FL	33437	*****	MA	NA	(11-01-1987)	kasahk	135	🛒 / +
ERLJO	32K	LAKE WORTH	FL	33481	*****	MA	NA	(11-01-1987)	kasahk	155	🛒 / +
SENELY TRANT	37K	BOCA RATON	FL	33487	*****	MA	NA	(11-01-1987)	kasahk	205	🛒 / +
NORMAN III	35K	POMPANO BEACH	FL	33060	*****	MA	NA	(11-01-1987)	kasahk	145	🛒 / +
DANIELLE	34K	LAKE WORTH	FL	33481	*****	MA	NA	(11-01-1987)	kasahk	145	🛒 / +
JACK	6K	BOCA RATON	FL	33487	*****	MA	NA	(11-01-1987)	kasahk	85	🛒 / +
JEFFREY	77K	BOCA RATON	FL	33487	*****	MA	NA	(11-01-1987)	kasahk	335	🛒 / +
ROVANN	34K	POMPANO BEACH	FL	33064	*****	MA	NA	(11-01-1987)	kasahk	145	🛒 / +
NELSON	33K	N LAUDERDALE	FL	33065	*****	MA	NA	(11-01-1987)	kasahk	155	🛒 / +
EDWARD	49K	BOCA RATON	FL	33487	*****	MA	NA	(11-01-1987)	kasahk	165	🛒 / +
CECIL	31K	MAHATE	FL	33568	*****	MA	NA	(11-01-1987)	kasahk	155	🛒 / +
GUSTAVO	27K	WEST PARK	FL	33023	*****	MA	NA	(11-01-1987)	kasahk	145	🛒 / +
FRANCINE	35K	PLANTATION	FL	33324	*****	MA	NA	(11-01-1987)	kasahk	155	🛒 / +
SHYLOK	7K	POMPANO BEACH	FL	33064	*****	MA	NA	(11-01-1987)	kasahk	85	🛒 / +
RANALFO	38K	POMPANO BEACH	FL	33064	*****	MA	NA	(11-01-1987)	kasahk	145	🛒 / +
MERLEJO	34K	MIAMI	FL	33181	*****	MA	NA	(11-01-1987)	kasahk	145	🛒 / +
ELIO	29K	OAKLAND PARK	FL	33334	*****	MA	NA	(11-01-1987)	kasahk	145	🛒 / +
SHARIE J	25K	POMPANO BEACH	FL	33063	*****	MA	NA	(11-01-1987)	kasahk	145	🛒 / +
SCHENRUS	35K	FORT LAUDERDALE	FL	33311	*****	MA	NA	(11-01-1987)	kasahk	145	🛒 / +
JUAN CARLOS	29K	POMPANO BEACH	FL	33064	*****	MA	NA	(11-01-1987)	kasahk	145	🛒 / +
ERRY	6K	BOCA RATON	FL	33489	*****	MA	NA	(11-01-1987)	kasahk	85	🛒 / +
MATTHEW	8K	WELLINGTON	FL	33414	*****	MA	NA	(11-01-1987)	kasahk	85	🛒 / +
SHEEMAH	83K	BOCA RATON	FL	33488	*****	MA	NA	(11-01-1987)	kasahk	205	🛒 / +

Showing 301 to 325 of 3607 entries (Filtered from 3607 total entries)

Page 10 of 120

Major Tax Preparer Accounts for Sale in the Underground

Logging out in: 98 min 47 sec

Main Accounts **Stuff** Cards Tutorials SMTP Purchased **Refill Balance** Tickets Profile Rules Sellers S. Rankings Logout

Search by Type Search by Country Choose your Reseller

Most Common Account
AliExpress AllBaba Apple Paypals Match Fedex Newegg
Netflix Ebay DHL Skype Overstock Macys UPS

Account Type	Country	Information	Reseller	Price	Buy
	Fresh	Account - Valid Login 100%	micro	5.00	<input type="button" value="Buy"/>
	Fresh	Account - Valid Login 100%	micro	5.00	<input type="button" value="Buy"/>
	Fresh	Account - Valid Login 100%	micro	5.00	<input type="button" value="Buy"/>
	Fresh	Account - Valid Login 100%	micro	5.00	<input type="button" value="Buy"/>
	Fresh	Account - Valid Login 100%	micro	5.00	<input type="button" value="Buy"/>
	Fresh	Account - Valid Login 100%	micro	5.00	<input type="button" value="Buy"/>
	Fresh	Account - Valid Login 100%	micro	5.00	<input type="button" value="Buy"/>
	Fresh	Account - Valid Login 100%	micro	5.00	<input type="button" value="Buy"/>
	Fresh	Account - Valid Login 100%	micro	5.00	<input type="button" value="Buy"/>
	Fresh	Account - Valid Login 100%	micro	5.00	<input type="button" value="Buy"/>
	Fresh	Account - Valid Login 100%	micro	5.00	<input type="button" value="Buy"/>
	Fresh	Account - Valid Login 100%	micro	5.00	<input type="button" value="Buy"/>

Meanwhile, back to the State Department of Revenue

- States saw a substantial increase in fraudulent returns and reports from taxpayers of ID theft and started implementing filtering techniques and solutions.
 - Fraud Manager (module within a state's integrated tax administration technology).
 - Uses certain fields on the return with prior history with the taxpayer to spot exceptions. Helpful but causes a lot of manual review. For example, a sign of possible fraud is using a different bank account from the prior year.
 - Retraining DOR employees from spotting good old fashioned tax cheaters to spotting new fangled identity theft situations.

All efforts helped but it was a SILO effort because each state was handling on their own and with no IRS involvement.

Use of External Sources to Authenticate the Taxpayer

- Data aggregators like Lexis Nexis or Thompson Reuters assist in legitimizing the taxpayer is the real taxpayer and not a criminal
 - Driver's License look up of the number, issuance date and expiration date
 - More communication with taxpayer when it is not clear if they are the real taxpayer
 - Can be a quiz asking for knowledge based answers based on credit history info from the bureaus or data aggregators
 - Answer questions online or by phone
- Pay refunds later to use the extra time to evaluate prior to paying refund
- Some are pricey but interagency cooperation is a must. Explore law changes if necessary to leverage the data housed in each agency.

Other Types of Fraud

- Tax Refund Fraud is the main issue, however...
 - Any agency that pays claims, benefits is a target
 - Blackmail
 - Employment fraud
 - Wire fraud
 - Money laundering (fraudulent refunds crossing state lines and U.S. borders)
 - Criminal conspiracies to defraud the government and to use financial institutions in facilitation of fraud
 - Bank fraud, mail fraud... etc., etc.
- Tax data is valuable to criminals!!

Even with States Stepping up Their Game...

- Working in a silo is never a great long term solution so states started working with a national association called the Federation of Tax Administrators (FTA) to pool ideas, share results, and collaborate.
- Early in the tax season in 2015, the nation's leading online tax software company was shutdown for varying periods of time by the IRS and most of the states due to the high volume of fraudulent returns reported.

WATERSHED MOMENT!

- The next month the IRS Commissioner formed the IRS Security Summit. This is the first time in history that the IRS, the States and the software tax prep companies were brought together to fight the fraud.

IRS Security Summit

- “This unprecedented partnership continues to put strong new safeguards in place for the 2016 tax season,” IRS Commissioner John Koskinen said. “We are breaking new ground in the battle against identity theft. Taxpayers will have more protection than ever when they file their tax returns.”

Targeted working groups have formed to address specific needs and are manned by subject matter experts from the IRS, State DOR and Private Sector companies. Is your state involved?

Fantastic results in just a short period of time

So far for 2017, individuals reporting identity theft have **declined sharply** compared to the same time in 2016 and 2015.

In the first five months of 2017, about 107,000 taxpayers reported being victims of identity theft, compared to the same period in 2016, when 204,000 filed victim reports.

That's about 97,000 fewer victims – representing **a drop of 47 percent**. For comparison, there were nearly 297,000 identity theft victims during the first five months of 2015.

<https://www.irs.gov/uac/newsroom/don-t-take-the-bait-step-3-security-summit-safeguards-help-protect-individuals-renew-focus-on-curbing-data-breaches-and-business-identity-theft>

Examples of Initiatives that Contributed to the Reduction

Multi-factor Authentication

credit karma | TAX

Verification

Verify your mobile number

If you sign in from a device we don't recognize, we'll text you a code to make sure it's you.

Mobile number

[Text me](#)

Standard call, messaging or data rates may apply.

Don't have a phone?
[Contact Member Support](#)

credit karma | TAX

Security | Verification

Enter verification code

[Verify](#)

Sent to (111)111-1111

The code expires after 5 minutes.

[Resend code](#)

ID Verification

Third party verification services



Other changes that have helped

- Delay paying refunds to allow more filtering techniques
- Driver's license real time validation
- W-2 Matching real time to ensure
 - Employee is reporting accurate wages
 - Employer actually remitted the funds
 - Mandating the W-2 copy sent to employee is sent to the DOR by end of January. What does your state law or regulation say about this? The Path Act mandated this to be sent to the IRS by 1/31.
- Internal ID Theft Fraud Units – civil and criminal charges
- Selfies or other biometric types of ID Validation. www.alabamaeid.com

Criminals Evolve as the IRS and States innovate

- W-2 Phishing Schemes are a great example. As the W-2 information was used as a new filtering tool, the criminals went on a nationwide frenzy to obtain as many as they could get to sell on the dark web. Most popular method was sending an email in the name of the CEO or other top executive asking for copies of the W2s to be emailed to them.
- **Don't Take the Bait!**
- <https://www.irs.gov/uac/newsroom/don-t-take-the-bait-step-3-security-summit-safeguards-help-protect-individuals>enew-focus-on-curbing-data-breaches-and-business-identity-theft

The fight to protect state and federal treasury dollars from criminals will evolve as the criminals adapt to our solutions, but with the new collaboration between state DOR's, the IRS and tax preparation software companies is making it harder and harder for criminals to profit from a fraudulent tax return.

Questions?