



**Understanding and Combating
Return Preparer Fraud
A Combined Effort**

Amy L. Hosney
Special Agent – Public Information Officer
IRS Criminal Investigation
Boston Field Office – New Haven POD




**Internal Revenue Service
Criminal Investigation Mission**

Criminal Investigation serves the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes in a manner that fosters confidence in the tax system and compliance with the law.




Refund and Cyber Crimes

- Return Preparer Program
- Questionable Refund Program
- Identity Theft
- Cyber Crimes




Return Preparer Fraud

- Preparation and filing of false income tax returns by unscrupulous preparers who:
 - Inflate personal or business expenses
 - Create false deductions
 - Excessive exemptions
- Preparers' clients may or may not have knowledge of the false expenses, deductions, exemptions and/or credits shown on their tax returns.




Investigative Approach

- Scheme Development
- Taxpayers and Informants
- Collaboration with other IRS Business Units




Criminal Violations

- Title 26 USC Section 7206(2)
- 18 USC 286 – Conspiracy to File False Claims (Tax-related)
- 18 USC 287 – Filing False Claims (Tax-related)
- 18 USC 641 - Theft of Government Funds
- 18 USC 510 – Treasury Check Charge
- 18 USC 1029 – Access Device Fraud
- 18 USC 1708 – Mail Theft
- 18 USC 1028 – Identity Theft




Education & Outreach

- Knock and Talk Visit Program
 - Special agents partner with revenue agents
 - Educational visits with return preparers
 - Identified by scoring system
- Field Office special agent visits
- Media Publicity/YouTube Videos
- Success measures




Return Preparer Program Statistics

Item	FY 2015	FY2016	FY2017	FY2018
Investigations Initiated	266	252	302	224
Prosecution Recommendations	238	174	193	177
Convictions	210	216	164	150
Conviction Rate	96.8%	98.6%	95.9%	96.8%
Sentenced	204	202	190	148
Avg. Months to Serve	27	22	26	25




Electronic Filing Identification Number

Item	FY 2015	FY2016	FY2017	FY2018
EFINs Suspended/Revoked	329	358	412	302




Warning Signs of Potential Fraud

- Income insufficient to cover claimed expenses
- Claiming false dependents
- Inflated itemized deductions including:
charitable contributions, medical or dental
expenses
- Claiming tax credits based on false
income/expenses
- False business expenses created to offset
income




Oversight of Emerging Threats

- Data Breaches
- EFINS/PTINS
- False/fraudulent ITINs




Information Security Evolving Threats

- Data Compromises/Computer Thefts
- Compromised Tax Professionals
 - Records used to generate ID theft claims mirroring actual taxpayer returns.
 - For 2017, 194 tax professionals (CPAs, enrolled agents, etc.) were compromised.
 - For 2018 (October 2017 to May 2018) 237 tax professionals were compromised.
- Compromised EFINS/PTINS



Information Security Evolving Threats (cont.)

- Payroll Web-portals
 - Involves payroll web-portals used by employees to access/view their W-2s, change payroll withholding, and other payroll information.
 - 5 to 7 business entities are compromised per day.
 - 1000's of clients
 - Ongoing investigations.
- Other Threats



News Releases

WASHINGTON – Seeing the emergence of a new filing season scam, the Internal Revenue Service today urged tax professionals to step up security and beware of phishing emails that can secretly download malicious software that can help cybercriminals steal client data.

Only a few days into the filing season, the IRS already identified a new scam that began with cybercriminals stealing data from several tax practitioners' computers and filing fraudulent tax returns.

In a twist, the fraudulent returns in a few cases used the taxpayers' real bank accounts for deposit. A woman posing as a debit collection agency official then contacted the taxpayers to say a refund was deposited in error and asked the taxpayers to forward the money to her.

This scheme is likely just the first of many that will be identified this year as the IRS, state tax agencies and tax industry continue to fight back against tax-related identity thieves. Because the Security Summit partners have made inroads against identity theft, cybercriminals have evolved their tactics to focus on tax professionals where they can steal client data.

Thieves know it is more difficult to identify and halt fraudulent tax returns when they are using real client data such as income, dependents, credits and deductions. Generally, criminals find alternative ways to get the fraudulent refunds delivered to themselves rather than the real taxpayers.

Internal Revenue Service
Criminal Investigation

From: sue@debtcredit.us
Date: January 30, 2018 at 3:05:32 PM PST
To: [XXXX](#)
Subject: OA6035

Dear XXXXX !
 My name is Sue Wang and i am your appointed debt collector from the DEBT & CREDIT CONSULTING SERVICES, LLC.
 I am here today regarding the following case - #OA6035
 It was noted that recently you received a money transfer in the amount of \$7656 on your REDWOOD CREDIT UNION account ending with 1477. However this money was accidentally sent to your account and you must return them.
 Please make sure that you visit the following link in order to resolve this issue:

http://debtcredit.us/case&case_id=OA6035

If you have any questions please do not hesitate to contact me.

Your Sincerely
 Sue Wang
www.debtcredit.us
 Tel: +1 877 364-6895
 DEBT & CREDIT CONSULTING SERVICES, LLC

Internal Revenue Service
Criminal Investigation

Welcome, Taxpayer Name | Case # 1234

Video Explainer

Glenn Adkins | Public Relations
 MANAGER


Case Information

Case #	1234
Debtor	Name
Amount	\$ 5919
Date	January 30, 2018

[DOWNLOAD RETURN SHEET](#)

Appointed debt collector

Name:	Sue Wang
Tel:	+1 877 364-6895
Email:	click to write me



Data reported from the IRS

Name	XXXXXXXXXX
SSN	XXX-XX-XXXX
DOB	XX/XX/XXXX

General Information
 You may be notified by an electronic document from the Internal Revenue Service but in fact it is sent an

Internal Revenue Service
Criminal Investigation

Protect

- Limit access to data and information
- Patch operating systems and applications
- Install/activate software and hardware firewalls on business networks
- Secure wireless access point and networks
- Set up web and email filters

Internal Revenue Service
Criminal Investigation xDedic Takedown



THIS DOMAIN HAS BEEN SEIZED

The domain for
xDedic

has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the Middle District of Florida under the authority of 18 U.S.C. § 981(b) as part of coordinated law enforcement action by:

Department of Justice
FBIHQ
U.S. Treasury
Florida State Police
federal prosecutor's office
Florida Department of Law Enforcement
Florida Highway Patrol
Florida Sheriff's Association
Europol



Internal Revenue Service
Criminal Investigation

xDedic Marketplace


- Jan. 2018 – Middle District of Florida announced seizure of the website.
- xDedic sold access to compromised computers worldwide and to PII of U.S. residents.
- Widely distributed network which utilized bitcoin to hide the locations of its servers and the identities of administrators, buyers, and sellers.
- The website facilitated an estimated \$68 million in fraud.
- Victims span the globe and all industries, including local, state, and federal government infrastructure, hospitals, 911 and emergency services, call centers, major metropolitan transit authorities, **accounting and law firms**, pension funds, and universities.
- Investigation led by FBI and IRS-CI.



Internal Revenue Service
Criminal Investigation


Mitigating the Breach

- Contact IRS Stakeholder Liaison When Compromise Detected
- <http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Stakeholder-Liaison-Local-Contacts-1>
- Contact Impacted State Tax Agencies
- https://www.irs.gov/businesses/small-businesses-self-employed/state-links-1?_ga=1.124839048.382356062.1475763178
- Federation of Tax Administrators at StateAlert@taxadmin.org
- Follow State Reporting Requirements (i.e. State Attorney General, State Consumer Protection Bureaus, State Police)
- File a complaint with the Internet Crime Complaint Center (IC3,) operated by the Federal Bureau of Investigation.
- Contact Local Police, US Secret Service, Other Law Enforcement
- Report Compromise to Federal Trade Commission
<https://www.identitytheft.gov/>



Internal Revenue Service
Criminal Investigation




Return Preparer Fraud Investigative Results



Internal Revenue Service
Criminal Investigation

BRIDGEPORT TAX PREPARER PLEADS GUILTY

- In April 2019, Rolando Russell pleaded guilty to two counts of aiding and assisting the filing of a false tax.
- Russell prepared approximately 1,820 tax returns for the 2013 - 2016 tax years through a tax return preparation practice he operated in Bridgeport.
- The returns claimed a total of approximately \$11.26 million in refunds, of which the IRS issued approximately \$10 million.
- Many of the returns included false Schedule C forms, Profit or Loss from Business.
- The losses attributed to Schedule C's totaled >\$22 million, resulting in a corresponding reduction of taxes owed of >\$6 million.
- For criminal purposes, Russell agreed to a tax loss of appx. \$1.5M.



Internal Revenue Service
Criminal Investigation


Guilty of stealing foster kids' identities, tax preparer gets 10 years in prison



Internal Revenue Service
Criminal Investigation

BERLIN MAN PLEADS GUILTY TO PREPARING FALSE TAX RETURNS




- On May 2nd, GELIN STERLING pleaded guilty to 1 count of 26-7206(2).
- Sterling owned Sterling Tax Plus, LLC, a tax preparation business.
- Client returns included false mileage expenses, charitable donations, & other false items.
- Sterling has agreed to pay restitution of \$250,000 to the IRS.
- Many of his clients' filed returns will need to be amended.
- Restitution may be reduced as clients resolve their own tax liability.



Internal Revenue Service
Criminal Investigation


NAUGATUCK TAX PREPARER INDICTED FOR FILING FALSE RETURNS


- In Dec. 2018, ANA NUNEZ was indicted on 12 counts of filing false tax returns.
- She operated Nunez MultiServices, LLC, a tax return preparation service.
- From 2011 through 2016, Nunez routinely inflated income or created fictitious income; falsified expenses, including education and child care expenses, and falsified deductions, such as business mileage.
- At times, without her clients' knowledge, Nunez also falsely inflated information on her clients' returns in order to increase their refunds and then directed the excess funds to an account she controlled.

Internal Revenue Service
Criminal Investigation


San Dimas Tax Preparer Sentenced to Prison for Filing False Returns




 Internal Revenue Service
Criminal Investigation

New London Tax Preparer Sentenced to Prison

- In Jan. 2019, Yves Aubourg was sentenced to 1 year in prison & ordered to pay \$219,180 in restitution.
- Operator of Providence Tax Services.
- Falsified thousands of tax returns from 2011 to 2015.
- The tax loss was \$264,870, resulting from the fabricated education & business expenses, dependents & charitable contributions.



 Internal Revenue Service
Criminal Investigation

