IRS Criminal Investigation

Special Agent R.J. Dawson
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.
Who are we and Where are we?

- Accountants
- Law Enforcement Officers – Criminal side of IRS
- 2100 Special Agents across the U.S.
- Big cities/small cities
- Judicial Districts
Types of Criminal Investigations

Title 26 – Tax Crimes
Title 18 – Fraud Crimes
North Carolina Businessman Sentenced to Prison for Stealing Approximately $2.9 Million from NFL Players

A Durham tax preparer who was convicted in January of preparing fraudulent tax forms for her and her clients was sentenced in federal court to 10 years in prison and was ordered to pay $1,742,823 in restitution to the Internal Revenue Service.

CF and PT, both from North Carolina, are charged with conspiracy to commit health care fraud, health care fraud, aggravated identity theft, and tax evasion. PT is also charged with one count of money laundering.
What IRS-CI Special Agents Do and do NOT Do

❖ Do – Investigative federal tax crimes
❖ Do not conduct tax audits
❖ Do not collect taxes
❖ Do not handle routine tax matters
❖ Not interested in people who make honest mistakes on their returns
Investigative Tools

- Trash/garbage pickups
- Search Warrants
- Seizure Warrants
- Undercover
- Consensual Monitoring
- Forensic Laboratory
- Surveillance
- Interviews
- Legal Orders – Subpoenas and Summons
Data Breaches Targeting the Tax Professionals and Business Email Compromises
Examples We are Seeing

❖ Gone before you had a chance

❖ Stolen Account info and wait for batching

❖ Stolen Account info and Erroneous Refund
From: sue@deburgeredit.us
Date: January 30, 2018 at 3:05:32 PM PST
To: XXXX
Subject: OA6035

Dear XXXX!
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://deburgeredit.us/case&case_id=OA6035

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

Your Sincerely
Sue Wang
www.deburgeredit.us
Tel: +1 877 364-6895
DEBT & CREDIT CONSULTING SERVICES, LLC
Signs of a Breach The Victim Experience

- Electronic Return Rejected (Paper Return)
- Verification Letters (5071C or 4883C)
- Receipt of US Treasury Refund Check
- Receipt of Reloadable Prepaid Card
- Receipt of Refund Transfer Company Check
Securing the Tax Pro

- Education (Tax Pros are not IT security Professionals)
- IT security Plans/Implementation
  - Logins-Passwords on Tax Software
    https://www.youtube.com/watch?v=opRMrEfAliI
  - Never Click on a Link
  - E-mails
  - Devices Connected/Access
- Anti Virus/Malware/Browser/Remote Access Software
- Multi Factor Authentication
- Biometrics
What is a Business Email Compromise (BEC)?

- The scam is carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

- The scam has evolved to include the compromising of legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees, and may not always be associated with a request for transfer of funds.
Cybercriminals are able to **identify** chief operating officers, school executives or others in position of authority (Social Engineering).

Fraudsters mask themselves as executives or people in authoritative positions and send emails to payroll or human resources requesting copies of Forms W-2. *(Grooming)*

Form W-2 contains the following *(Exchange of Information)*

- Employment Identification Numbers (EIN)
- Social Security Numbers
- Income / Withholdings (Federal, State, Local)
- Address
- Retirement Plan
- Health Benefits Plan
❖ The e-mail correspondences usually contain grammar and spelling errors.

❖ The data compromises usually go undetected for over 210 days.

❖ Information is usually sold on Dark Web to other groups.
How Can I Help Protect My Company?

- **Do not use the “Reply” option** to respond to any business e-mails asking for PII
- Educate your employees
- Be careful what you post to social media and company websites
- Be suspicious of requests for secrecy or pressure to take action quickly
- Carefully scrutinize all e-mail requests for PII or financial transactions
Mitigating the Breach

- Contact IRS Stakeholder Liaison When Compromise Detected
  - For NC call (412) 404-9151 (Area 4)
- Contact Impacted State Tax Agencies
  - NC Department of Revenue
  - Division of Employment Security
  - 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/](https://www.identitytheft.gov/)
Actions When Compromised

Payroll Related Compromises

❖ Organizations who actually lost W-2 information via a scam email should e-mail IRS via dataloss@irs.gov and follow instructions.

❖ Organizations who did not actually lose W-2 information via a scam email should e-mail IRS via phishing@irs.gov and follow instructions.

❖ Lost Payroll data can impact State Agencies as well. Victims should email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report States Tax Agencies.

❖ Follow State Reporting Requirements (i.e. State Attorney General, State Consumer Protection Bureaus, State Police)

❖ Organizations that receive the scam or fall victim to them should file a complaint with the Internet Crime Complaint Center (IC3,) operated by the Federal Bureau of Investigation.

❖ Contact Local Police or Other Law Enforcement

Basic Requirements:
- United States citizen
- Age 37 or under at the time of certification
- Bachelor’s degree – with 15 semester hours of accounting and 9 hours of related business
- Available to work anywhere in the US
- Must carry and use a firearm
- Have a valid driver's license
- Pass an agency-administered physical fitness test*