

The IRS Under Trump:

What It Means for Tax and Accounting Professionals

Eric Green
Sam Schuemacher

TRN
TAX REP NETWORK

Speakers



Muppet Eric and Sam



Housekeeping

- ▶ 4 Polling Checks
- ▶ Please respond for ce/cpe
- ▶ If you do a link will be sent to claim your certificate
- ▶ EAs put your PTIN number in for reporting to the IRS
- ▶ Issues? Email us at team@taxrepllc.com



Agenda



1. DOGE is remaking the IRS
2. Automation will rule the day
3. Data thieves are going to target the weak link - practitioners

Trump, DOGE and the IRS: Chaos



End of the IRS?



Where are we right now?

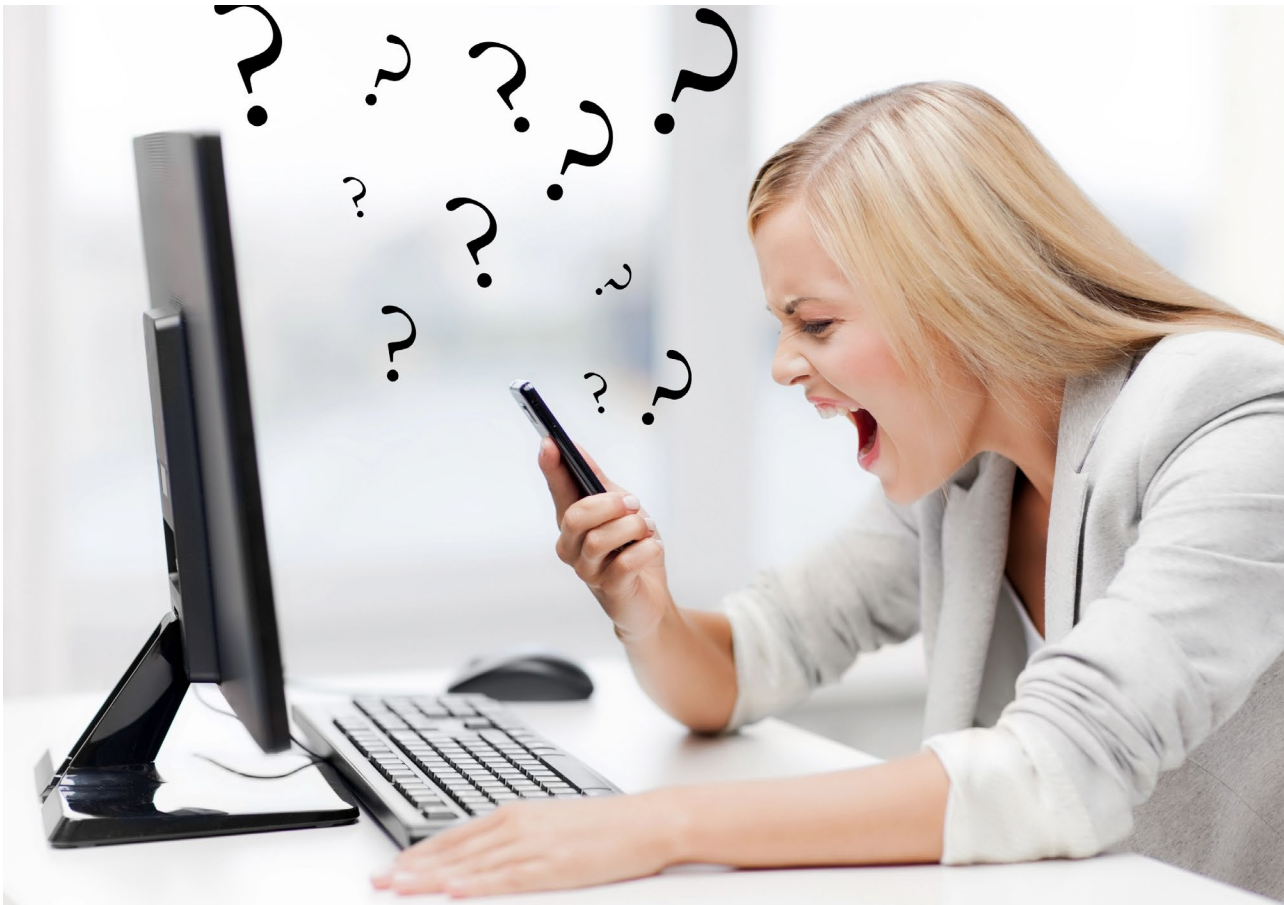
- ▶ 11.3 Million Non-filers
- ▶ Over 15 million with balances due
- ▶ Automated enforcement began again in 2024 (AUR, ASFR, Automated Liens and Automated levies)



Where we are....

- ▶ 11% of the IRS workforce let go, including 2,000 people who answered the phones
- ▶ 1/3 of offices being closed, including Taxpayer Assistance Centers
- ▶ Net result: good luck getting someone on the phone

Have you called the IRS lately?



Taxpayer



IRS

Acting Commissioner of the Week

- ▶ IRS Acting Commissioner Bessent confirms the IRS plans to use A.I. to close the gap from the workforce reduction and expects collections and enforcement to continue to be robust through the use of Artificial Intelligence and automation.
- ▶ “I would expect that collections would continue to be very robust as they were this year.”

- ▶ Everything shifting to automation
- ▶ DOGE told our folks at the executive level that instead of cases (audits and collection) waiting in queue they can now all be worked simultaneously
- ▶ The portals continue to be an issue....
- ▶ Future of working with the government is online

What this adds up to

The easiest target for data thieves to access tax info is....
you, the tax pro!



How many of you have a WISP: Written
Information Security Plan?

Query:

How many of you renewed your
PTIN for this year (2025)?

PTIN renewal check box

Data Security Responsibilities – remember checking this box on your renewal?

“As a paid tax return preparer, I am aware of my legal obligation to have a data security plan and to provide data and system security protections for all taxpayer information. Check the box to confirm you are aware of this responsibility.”

You are REQUIRED to have a WISP

- ▶ Written Information Security Plan
- ▶ You need to train your staff to recognize phishing schemes and not open attachments sent (No I did not ask for apple gift cards)
- ▶ It should match what you are doing (i.e. a canned plan will not help you if it becomes necessary to defend yourself before the FTC or IRS OPR)

The Security Six

1. Anti-Virus Software
2. Firewalls
3. Two-Factor Authentication
4. Back-up Software or Services
5. Drive Encryption
6. Virtual Private Network

Agenda

- ▶ Indicators of a data breach
- ▶ The fallout of failing to inform the IRS of a data breach
- ▶ IRS resources that can assist tax professionals in securing their tax data



Recognize the signs of client data theft

- ▶ Tax professionals should learn the signs of a possible data theft
- ▶ Data theft may result in fraudulent tax returns being filed in their clients' names
- ▶ Cybercriminals are tax savvy in their attempts to gain sensitive tax data

Signs of Client Data Theft

- ▶ Client e-filed returns begin to reject;
- ▶ Clients who haven't filed tax returns begin to receive authentication letters (5071C, 4883C, 5747C) from the IRS;
- ▶ Clients who haven't filed tax returns receive refunds;

Signs of client data theft (cont.)

- ▶ Clients/Practitioners receive tax transcripts that they did not request;
- ▶ Clients who created an IRS Online Services account are notified that their account was accessed or disabled
 - Another variation: Clients receive notice that an account was created in their names

Signs of client data theft (cont.)

- ▶ The number of returns filed with tax practitioner's Electronic Filing Identification Number (EFIN) exceeds number of clients;
- ▶ Tax professionals or clients responding to emails that practitioner did not send

Signs of client data theft (cont.)

- ▶ Network computers running slower than normal;
- ▶ Computer cursors moving or changing numbers without touching the keyboard;
- ▶ Network computers locking out tax practitioners.

Tax professionals monitor your accounts

- ▶ EFIN accounts
 - ❑ Too many returns filed with your EFIN
 - ❑ Contact e-Help Desk (866) 255-0654
- ▶ PTIN accounts
 - ❑ Too many returns filed
 - ❑ Complete Form 14157
- ▶ CAF accounts
 - ❑ Signs of identity theft
 - ❑ Contact Practitioner Priority Service

Step 5: Create a data theft recovery plan

- ▶ An action plan can save valuable time and protect your clients and yourself
- ▶ Make calling the IRS an immediate action item

Data Compromise Action Items – Report immediately

Contact:

- ▶ IRS Stakeholder Liaison. Search “stakeholder liaisons” on IRS.gov
- ▶ Contact experts
 - ❑ Insurance company
 - ❑ Computer security experts
- ▶ Law enforcement

Data Compromise Action Items – Report immediately (cont.)

Contact state agencies:

- ▶ State revenue agencies - email Federation of Tax Administrators for state agency contacts at StateAlert@taxadmin.org
- ▶ State Attorneys General

Data Compromise Action Items – Report immediately (cont.)

Contact:

- ▶ FTC for guidance for businesses

- Email: idt-brt@ftc.gov

- ▶ Credit Bureaus

- ▶ Clients

Review guidance at [IRS.gov/identitytheft](https://www.irs.gov/identitytheft)

Did You Know?

- ▶ As of May 13, 2024, if you have a data breach that impacts 500 or more clients you are REQUIRED to inform the FTC no more than 30 days after the discovery of the breach
- ▶ The maximum civil penalty is \$53,088 for 2025 (indexed for inflation)

**Have you implemented a
software solution for
your cyber security?**

Dealing with this

- ▶ My IT security is like a car – I can drive it but I have no idea how it works
- ▶ I don't want to be an IT consultant
- ▶ I'm not hiring a CIO



- ▶ Risk assessments, tailored security policies, and ongoing management
- ▶ Secure compliance
- ▶ WISP done, tailored for your company
- ▶ Multifactor Authentication (MFA)
- ▶ Secure Access Service Edge (SASE)
- ▶ Private Cloud and Application Hosting
- ▶ Secure Cloud Drive



Questions

Eric Green: egreen@gs-lawfirm.com

Sam Schuemaker - sschuemaker@visory.net

Mandy Sullivan - msullivan@visory.net

