IRS Updates

Richard Furlong, Jr.
Senior Stakeholder Liaison

Accountant-Lawyer Alliance Webinar
November 25, 2025

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Snapshot Report: IRS Workforce Reductions as of March 2025

May 2, 2025

Report Number: 2025-IE-R017

IRS Workforce

103,000 Employees
as of February 2025

-11%

7,315
Probationary Employees Who Received Termination Notices

4,128
Deferred Resignation Approvals

Top Six IRS Business Units Affected by IRS Separations

Description of IRS Business Units

Human Capital Office (HCO) supports IRS employee with Human Resource topics.

Information Technology (IT) supports IRS employees by delivering IT services and solutions.

Large Business and International (LB&I) helps corporations, partnerships with assets greater than $10 million to comply with tax laws, including emerging international issues.

Small Business/Self Employed (SB/SE) helps small business and self-employed taxpayers understand and meet their tax obligations.

Tax Exempt & Government Entities (TE/GE) helps taxpayers with pension plans, exempt organizations, and government entities to comply with the tax laws.

Taxpayer Services (TS) helps taxpayers understand and comply with tax laws.

Snapshot Report: IRS Workforce Reductions as of March 2025

Figure 3: Count and Percentage Impact of Separations on the Top 6 IRS Business Units

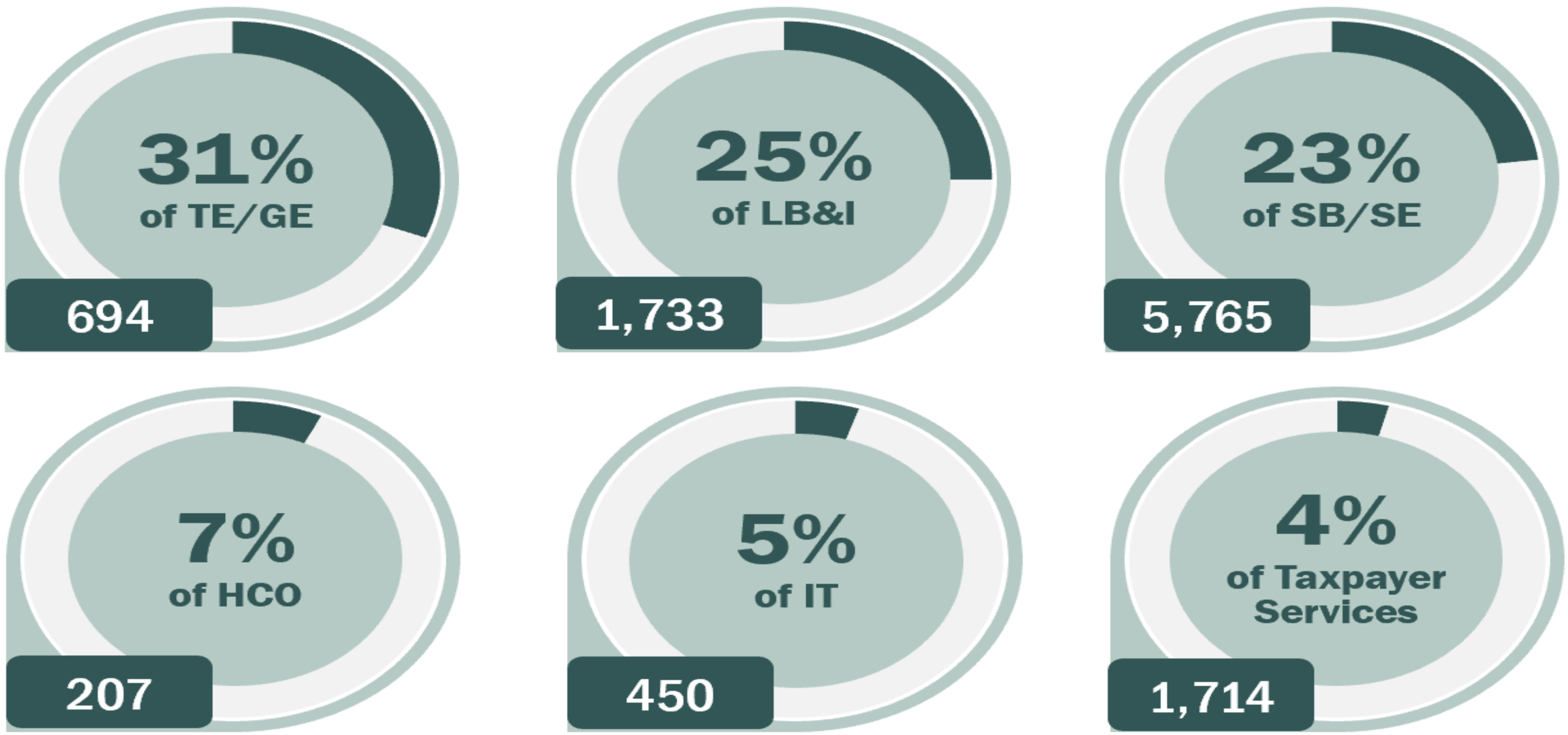


Figure 4: Top 6 Job Series Most Affected by IRS Separations

Brief Description of Job Titles

Contact Representatives helps taxpayers resolve their tax-related issues.

IT Management supports information technology (IT) systems and services.

Miscellaneous Clerical and Assistants provide administrative support for IRS operations.

Revenue Agents examine tax returns to determine or advise on liability for Federal tax laws.

Revenue Officers perform work related to collecting delinquent taxes, surveying for unreported taxes, and securing delinquent returns.

Tax Examiners perform work related to processing tax return, managing accounts, collecting taxes and/or obtaining tax returns, computing or verifying tax, penalties, and interest, and determining proper tax liabilities.

Snapshot Report: IRS Workforce Reductions as of March 2025

Figure 5: Count and Percentage Impact of Separations by Job Series

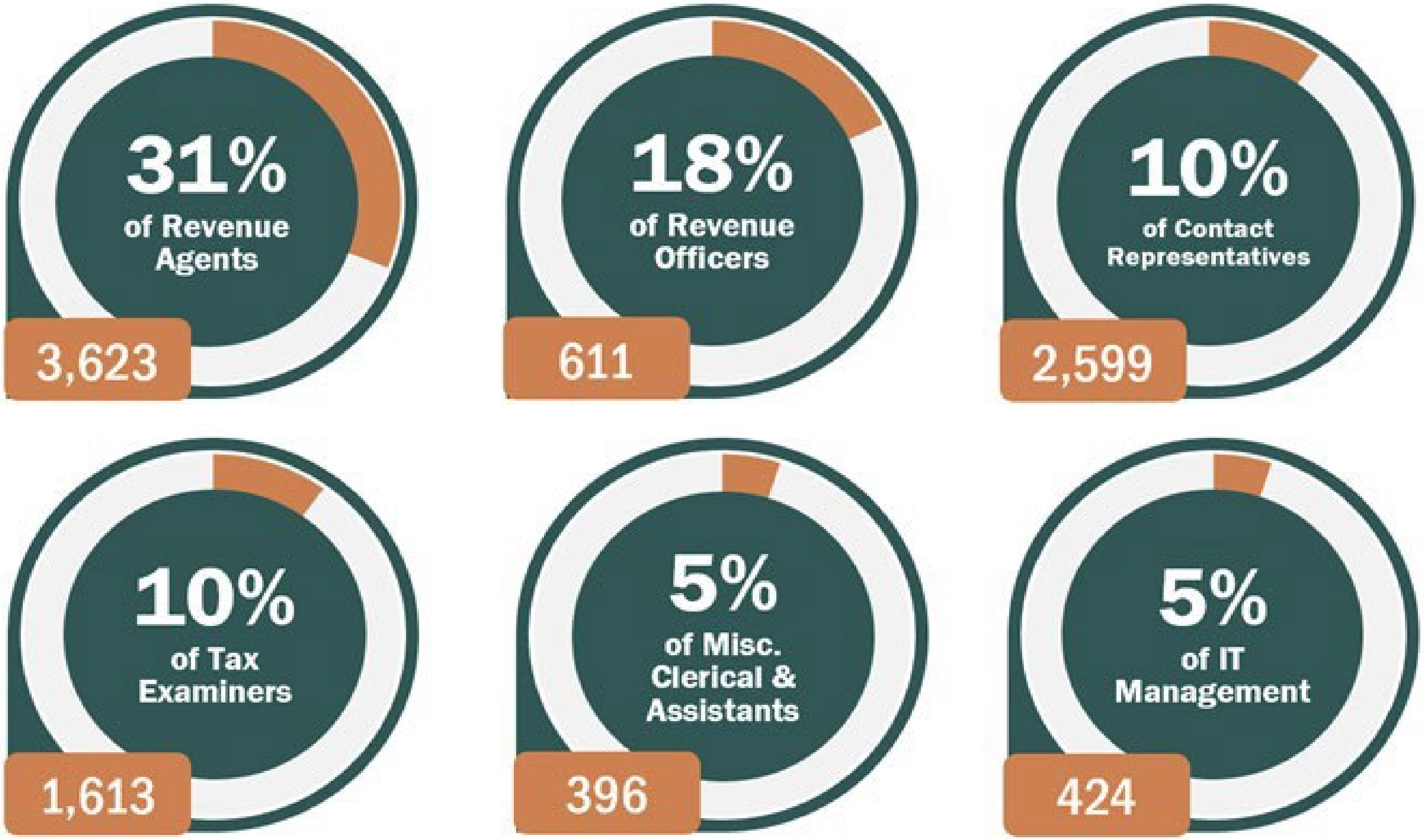
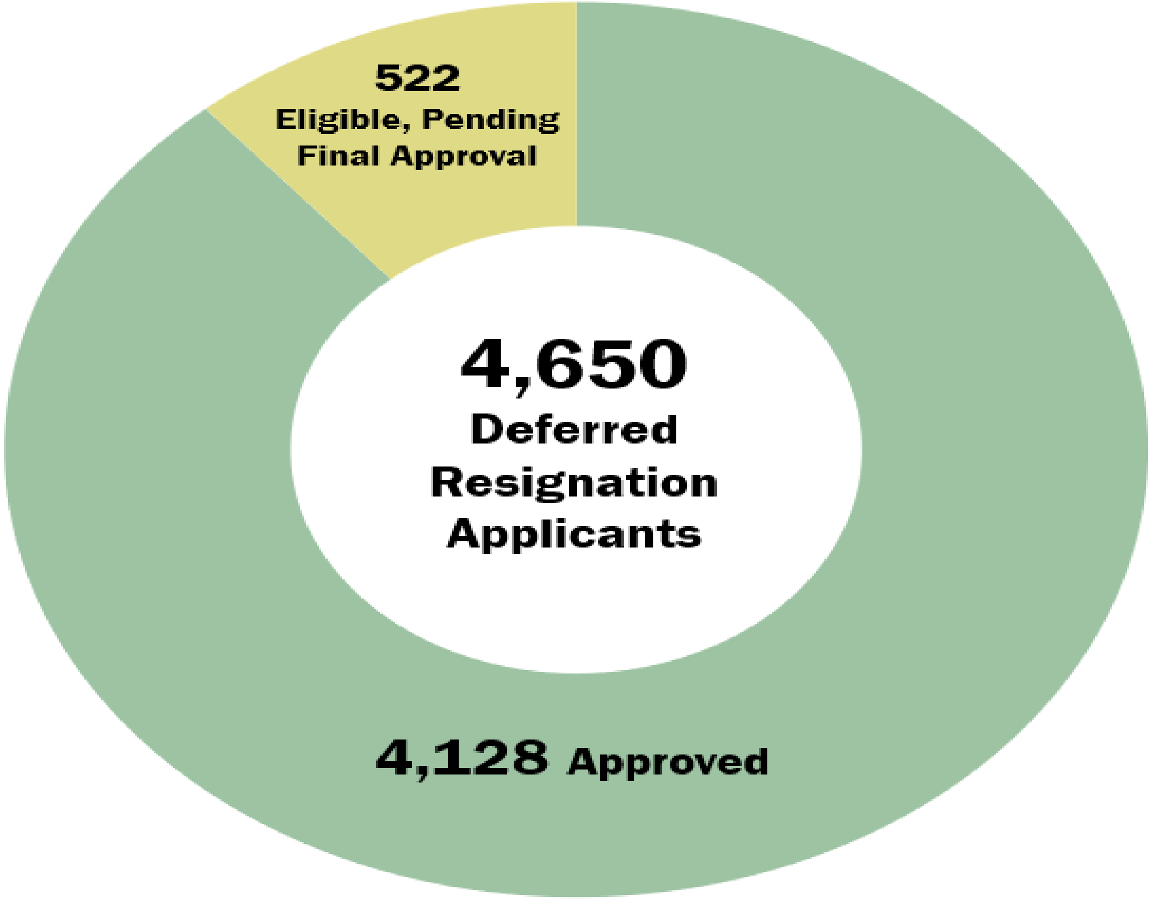


Figure 8: Status of DRP 1.0 Approvals and Pending Eligibility



Treasury Deferred Resignation Program 2.0

As previously mentioned, in April 2025, the IRS extended the TDRP offer to its employees. According to the IRS, **over 23,000 employees applied for the TDRP, and 13,124 were approved as of April 22, 2025**. We will continue to report on the impact of the TDRP and RIF procedures on the IRS workforce in subsequent reports.

May 30, 2025
Executive Order 14247:
"*Modernizing Payments To and From America's Bank Account*"

Transitioning federal disbursements to electronic payments

Executive Order (E.O.) 14247, Modernizing Payments to and from America’s Banking Account

Current State & Drivers for Change

The IRS has been working to reduce paper tax refund payments for several years. The Executive Order is accelerating those efforts.

Historically for those taxpayers filing tax returns:

- 91.5% of individual taxpayers file with banking/direct deposit information
- 4% of businesses receive a direct deposit

About 800,000 direct deposits are rejected by financial institutions annually.

The IRS is focusing efforts to help taxpayers in this filing population, as well as those who are unbanked, to successfully submit banking information.

Transition Execution & Communication Framework

The IRS is:

- **Changing business tax return forms to include fields for direct deposit information.**
- **Communicating via press releases, FAQs, content on IRS.gov and more to keep the public updated as we move toward January 2026.**
- **Leveraging the tax industry, software providers and tax practitioners to amplify messages on what to expect.**
- **Partnering with Bureau of Fiscal Service on new or updated tools for the diverse demographics of IRS customers.**
- **Expanding refund options for IRS customers to include:**
    - ➢ Direct deposit to checking or savings accounts.
    - ➢ Use of reloadable debit cards.
    - ➢ Use of accounts associated with digital payments.

Future State & Priorities

<u>**Key Changes Starting in January 2026:**</u>

Businesses and Individuals should provide direct deposit information when tax returns are filed.

The IRS will send letters to individuals asking them to update their banking information if they do not provide it on their tax return, or if a direct deposit has been rejected by their financial institution.

If their banking information is missing when filing electronically, the individual will receive an alert or message. The tax return will still be accepted and processed.

- The taxpayer will receive a notice requesting banking information <u>or</u> a reason it cannot be provided within 30 days. In addition, Where's My Refund will provide messaging associated with the need for banking information. The taxpayer can use the Individual Online Account to provide their information.
- A tax refund will be held for up to 6 weeks from when the tax return is processed in our system. Once the taxpayer provides the direct deposit information or exception, the refund will be immediately released via direct deport or paper check. After 6 weeks, the refund will be released as a paper check, if there are no other issues with the tax return.
- Individual Online Account will be expanded to capture the banking information or reason for an exception for those receiving a notice.
- IRS will have a phone extension for taxpayers to provide an exception, if Individual Online Account is not an option.
- Customer Service Representatives **cannot take direct deposit information** over the phone or in-person.

Future State & Priorities Contd.

There are multiple options for most individual taxpayers to receive direct deposits. The IRS and Treasury will continually promote resources for opening a free or low-cost account by visiting FDIC: GetBanked and MyCreditUnion.gov for account options.

Many of the tax software companies and practitioners offer reloadable debit cards. This may be an option for some taxpayers.

The Future Beyond 2026:

- **Opportunities to have similar processes for those individuals filing amended tax returns.**
- **Improve access and work around International refunds and access to digital payments.**
- **Incorporate any learnings from 2026 to improve the experience and expand direct deposit activities further in 2027.**
- **Possible updated guidance in the Summer of 2026. Stay tuned on IRS.gov and published material.**

2025

IRS DIRTY DOZEN:

Tax Scams & How to Avoid Them

IRS Dirty Dozen Tax Scams

Email Phishing Scams

Bad Social Media Advice

IRS Individual Online Account "Help" from Scammers

Fake Charities

False Fuel Tax Credit Claims

Credits for Sick Leave and Family Leave

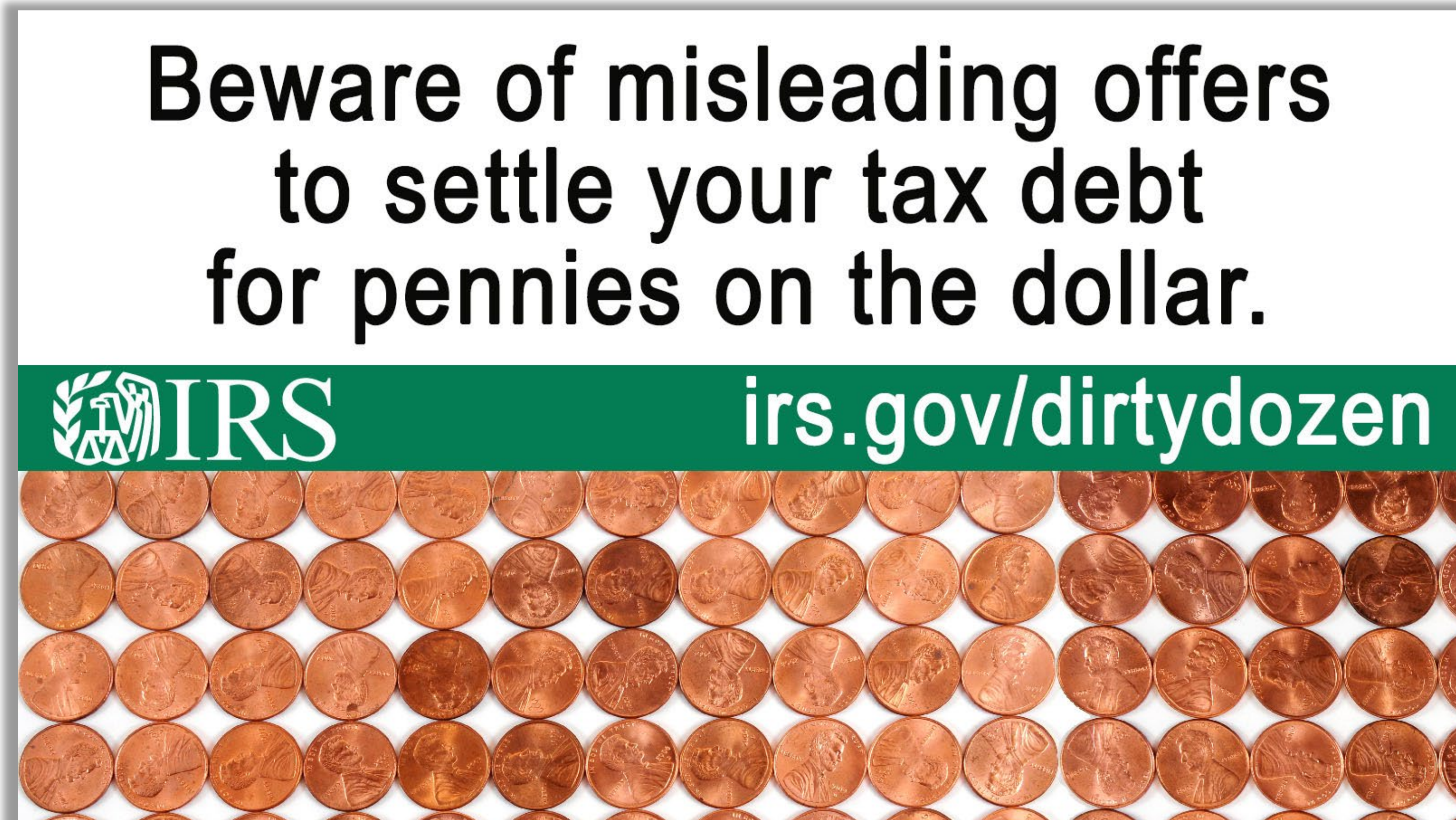
Bogus self-employment tax credit

Improper household employment taxes

2
5

The Overstated Withholding Scam

Misleading Offers in Compromise



Ghost Tax Return Preparers

New Client Scams and Spear Phishing

Watch Out for Other Abusive Schemes

Recovering from a Scam: Protecting Finances

- Immediately stop interacting with the scammer
- Don’t send money or share personal information
- Contact financial institutions

Recovering from a Scam: Protecting Tax Information

- Get an Identity Protection PIN (IP PIN)

- **Set up an IRS tax account**
  - Accounts are available for:
    - Individuals
    - Businesses
    - Tax professionals

- Monitor the IRS tax account activity

Recovering from a Scam: Report Loss of Identity

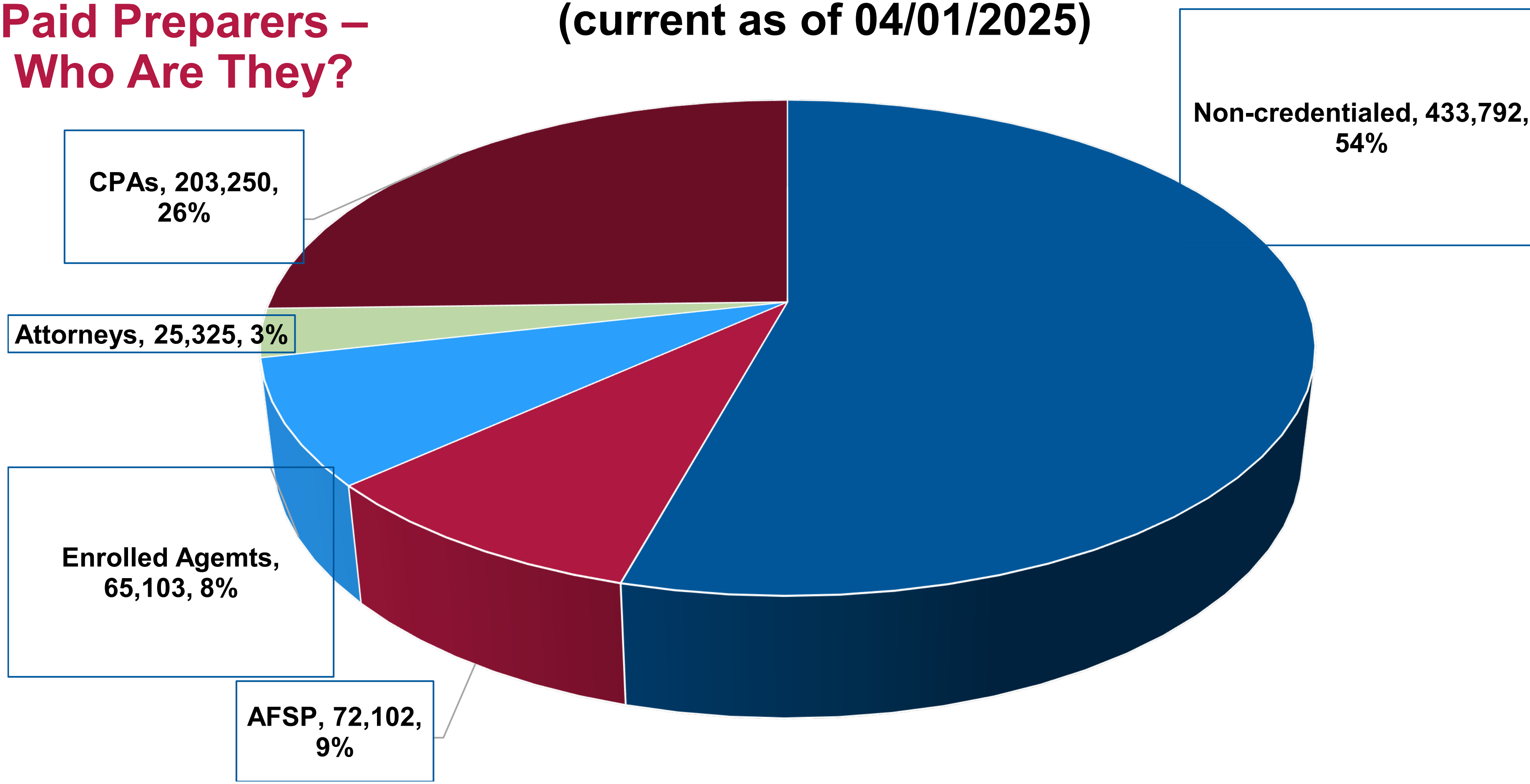
- If a taxpayer's Social Security Number (SSN) or Individual Tax Identification Number (ITIN) was stolen, report it to:
  - IdentityTheft.gov
  - IRS by submitting Form 14039, Identity Theft Affidavit
  - Their state tax agency

- Visit IRS.gov/scams
- Complete Form 14242, Report Suspected Abusive Tax Promotions or Preparers
  - Submit online

    or
  - Mail/fax to the IRS Lead Development Center

Paid Preparers – Who Are They?

800,201 ACTIVE PTINs (current as of 04/01/2025)



Tax Professional Data Breaches and How Tax Pros Can Protect Themselves

Deploy the "Security Six" Protections:

1. Anti-virus software
2. Firewalls
3. Two-factor authentication
4. Backup software/services
5. Drive encryption
6. Virtual Private Network (VPN)

BEWARE OF SPEAR PHISHING

Phishing Lifecycle

A Lure: enticing email content

A Hook: an email-based exploit (e.g., a phishing URL or malicious attachment)

A Catch: a transaction conducted by an actor following a successful attempt

“New Client” Scam 1st Email

From: [REMOVED]

To: [TAX PREPARER]

Sent: Thu, Apr 21, 2022 3:06 pm

Subject: Extension Client Intake

Good Morning,

I am [REMOVED], married, father of three teenage boys and a business owner. My family and I have lagged behind in filing our taxes and I am hoping you are not at capacity and willing to take on a new client? I have all by books and forms in place, don't owe taxes and usually make estimated tax payments.

Please write back if you are open to new tax clients and how to proceed. Regards[REMOVED]

“New Client” Scam 2nd Email

From: [REMOVED]

To: [TAX PREPARER]

Sent: Wed, May 4, 2022 6:14 am

Subject: Re: Extension Client Intake

Hi [TAX PREPARER],Sorry for the late response, things haven't been going as planned lately. I won't want to bore you with personal issues. As for my taxes, I usually don't owe taxes, applied my prior year refund and also made estimated tax payments to cushion effects of situations like these.

**[REMOVED]_1040_ScanCopy.pdf*

*<hxxps://example[.]example/file/[REMOVED]>**

Above is a secure and SSL excerpted copy of my prior year returns for your perusal. Kindly review and advise on way forward... I look forward to talking with you.Regards[REMOVED]

IRS, Security Summit partners warn of surge in "new client" scams aimed at tax pros as 2024 filing season approaches

IR-2024-05, Jan. 9, 2024

WASHINGTON – The Internal Revenue Service and the Security Summit partners today alerted tax professionals to watch out for a new round of filing season-related email schemes where cybercriminals pose as potential clients.

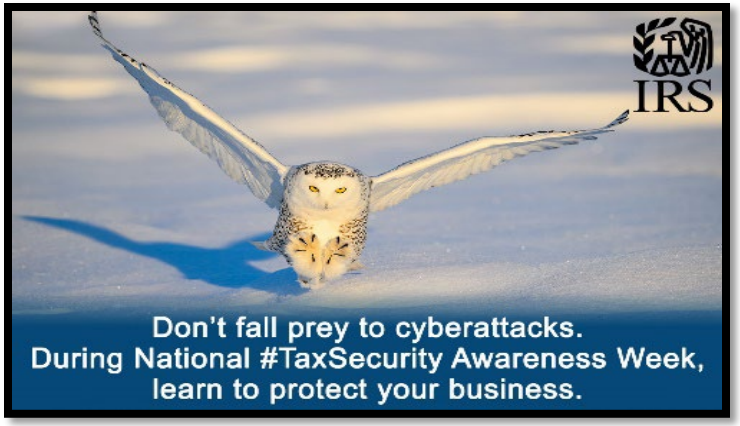
Previously, the IRS observed a surge in these seasonal "new client" scams where identity thieves target accounting groups and tax preparation firms with fake emails. This year, the IRS has already observed reports of new client scams. Typically, the new client scam peaks during tax season, which runs from January through April. With the 2024 tax season quickly approaching, fraudsters are impersonating real taxpayers seeking help with their taxes, using emails to try obtaining sensitive information or gain access to tax professionals' client data.

Tax Pros Stay Safe by having a WRITTEN INFORMATION SECURITY PLAN (WISP)

Pub 5461-D Tax professionals should review their security protocols
Pub 5461-F Review account details on secure portal

- Develop a WISP
- Use IRS Secure Online Tools (Tax Pro Account)
- Use Multi-Factor Authentication
- Know what to do if you have a Data Breach
- **Pub 5708** Creating a WISP
- Nov 30 WISP Webinar

Businesses Stay Safe by SAFEGUARDING INFORMATION



Pub 5461-C Businesses should watch out for tax-related scams and implement safeguards

- Safeguard customer data
- Beware of phishing and impersonation schemes
- Review tips in the business section of Identity Theft Central on IRS.gov

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

IRS, Treasury and/or tax-related phishing scams:

Please send full email headers to phishing@irs.gov

If you click on a nefarious link, download a document, etc.: Contact Your Tax Software Provider

Tax preparers who experienced a data breach:

Contact Stakeholder Liaison (SL): (www.irs.gov search "*Stakeholder Liaison*")

TIGTA.gov

FTC.gov or IdentityTheft.gov

IRS Publication 4557(“*Safeguarding Taxpayer Data”*) – download at IRS.gov

***“Small Business Information Security – The Fundamentals”* – *download* at NIST.gov**

Subscribe to e-News for Tax Professionals

Creating a Written Information Security Plan for your Tax & Accounting Practice

IRS Publication 5708

Creating a Written Information Security Plan (WISP) for your Tax & Accounting Practice

This document was prepared by the Security Summit, a partnership of the Internal Revenue Service, state tax agencies, private-sector tax groups as well as tax professionals. The mission of the Security Summit is to fight identity theft and tax refund fraud.

This document is intended to provide sample information and to help tax professionals, particularly smaller practices, develop a Written Information Security Plan or WISP. It is not an exhaustive discussion of everything related to **WISPs and it is not intended to replace your own research, to create reliance or serve as a substitute for developing your own plan based upon the specific needs and requirements of your business or firm.** A written information security plan is just one part of what tax professionals need to protect their clients and themselves. Given the rapidly evolving nature of threats, the Summit also strongly encourages tax professionals to consult with technical experts to help with security issues and safeguard their systems.

There are many aspects to running a successful business in the tax preparation industry, including reviewing tax law changes, learning software updates, and managing and training staff. Creating a Written Information Security Plan or WISP is an often overlooked but critical component. Not only is a WISP essential for your business and a good business practice, the law requires you to have one. For many tax professionals, knowing where to start when developing a WISP is difficult. This guide provides multiple considerations necessary to create a security plan to protect your business, and your clients and comply with the law.

WISP - Outline

The bare essentials of a Written Information Security Plan are outlined below. Be sure you incorporate all the required elements in your plan, but scale the comprehensiveness to your firm's size and type of operation. The elements in the outline are there to provide your firm a narrower scope of purpose and define the limitations the document is meant to cover. Therefore, many elements also provide your firm with a level of basic legal protections in the event of a data breach incident. For a detailed explanation of each section, please review the detailed outline provided in this document.

I. Define the WISP objectives, purpose, and scope

II. Identify responsible individuals

- a. List individuals who will coordinate the security programs as well as responsible persons.
- b. List authorized users at your firm, their data access levels, and responsibilities.

III. Assess Risks

- a. Identify Risks
  - List types of information your office handles
  - List potential areas for data loss (internal and external)
  - Outline procedures to monitor and test risks

IV. Inventory Hardware

- a. List description and physical location of each item
- b. Record types of information stored or processed by each item

Data Security

- Cybercriminals continue to target tax professionals. There is a heightened need for security as fraudsters seek to use phishing, remote takeovers, and other sophisticated techniques to scam taxpayers and tax professionals. Protecting yourself against cybercrime is essential in today’s digital age.
- Increase your level of awareness about identity theft and data security measures.
- Be mindful of your responsibility to protect client data.
- By following some simple steps and staying vigilant you can reduce the risk of falling victim to cybercrimes and protect yourself and your clients against online threats.

Safeguarding Taxpayer Data

- **Federal Trade Commission (FTC) Safeguard Rules require financial institutions (paid tax return preparers fall within the definition of financial institution) to create and maintain security plans to protect client data.**
  - **Amendment to Safeguards Rule**
    - Requires financial institutions to notify FTC as soon as possible – and no later than 30 days after discovery that information affecting 500 or more people has been acquired without authorization

Safeguarding Taxpayer Data (cont.)

- **Tax Return Preparer roles/responsibilities:**
  - Restrict access and disclosure to authorized staff
  - Plan appropriate safeguards/security controls
  - Designate safeguard responsibilities
  - Monitor, evaluate, adjust security plan periodically

When You (WISP) Upon a Star

A written information security plan or WISP is an essential step in protecting your business against data loss and tax related identity theft. While plans should be tailored to your office, here are some basics for all tax pros:

- **IDENTIFY** and assess all risks to Personally Identifiable Information (PII) (e.g. names, addresses, email addresses, bank information).
- **EVALUATE** the effectiveness of current safeguards for controlling risks to data. Review internal controls such as anti-virus software, data encryption, use of strong passwords, and limiting access to taxpayer data to those who need to know.
- **DESIGN** a data security program to protect data and business systems. Cybersecurity professionals can help customize a security plan appropriate for the business's size, activities, and customer information.

When You (WISP) Upon a Star

- **IMPLEMENT** safeguards and recommendations of the cybersecurity professional. Ensure security software is being used client data is being protected and know how to recognize data theft.
- **MONITOR** and test safeguards after design and implementation of security plan and adjust the plan as time goes on. WISP is intended to be an evergreen document that is regularly reviewed and updated
  - **Remember to monitor EFINs/PTINs, system and business operations regularly.**

Storing a copy of your WISP offsite or in the cloud is a recommended best practice in the event of a physical disaster.

You’ve Been Breached! What Next?

If you experience a data breach, here’s how to report your data loss:

Contact the IRS and law enforcement:

- Report client thefts to your local IRS Stakeholder Liaison (SL will notify IRS Criminal Investigation (CI) and others within the agency on your behalf
- Federal Bureau of Investigations (FBI), local office (if directed by IRS)
- Secret Service, local office (if directed by IRS)
- Local police department to file a report
- File a report with the FTC if you have 500 or more people that have been affected.

You’ve Been Breached! What Next? (cont.)

Contact the states in which you prepare returns:

- Visit the Federation of Tax Administrators “Report a Data Breach” webpage to find state contact information at: **Taxadmin.org/report-a-data-breach**
- Attorney General (AG) for each state you prepare returns – most states require that the AG be notified of data breaches

Contact experts:

- Security expert – to determine cause/scope of breach, stop the breach and prevent future breaches
- Insurance company – to report breach and determine policy coverage

You've Been Breached! What Next? (cont.)

Contact clients and other services:

- Clients – send letters to all victims informing of the breach
- Federal Trade Commission – can assist businesses victimized by data thefts, including resources on notifying clients
- Credit/ID theft protection agencies – some states require offering credit monitoring/ID theft protection to victims
- Credit bureaus – notify them of data compromise since clients may seek their services

Implement Best Security Practices

- Learn to recognize and avoid phishing emails and phishing scams
- Be careful of email attachments and web links
- Use strong security software to protect against malware and viruses
- Encrypt taxpayer data and use strong VPNs (Virtual Private Networks)
- Use strong, unique passwords
- Use separate personal and business computers, mobile devices, and email accounts
- Watch for harmful pop-ups
- Be careful downloading software
- Do not connect personal or untrusted storage devices or hardware into computers, mobile devices, or networks

Use Available Security Resources

- Publication 4557, Safeguarding Taxpayer Data
- Publication 5708, Creating a Written Information Security Plan for Your Tax & Accounting Practice
- National Institute of Standards and Technology (NIST) Publication 7621 – Small Business Information Security – The Fundamentals
- e-News for Tax Professionals (good source of information on latest threats and scams)
  - **IRS.gov keyword search "e-news subscription"**

A Little Something Extra

Modernization Efforts

- IRS/RPO continues to focus on modernizing its systems and processes to improve the tax preparation experience for taxpayers and tax professionals.

- If you're a tax return preparer and discover that another preparer is committing any of the practices on the next slide, submit a complaint using the online mobile-friendly version of **Form 14157, *Return Preparer Compliant*.**

Form 14157, *Return Preparer Complaint*

Form 14157 can now be completed and submitted online.

- Report improper tax preparation practices
- Failure to enter PTIN on a tax return or using an incorrect PTIN
- Failure to sign tax returns one has prepared or filed
- Falsely claiming to be a CPA, attorney, enrolled agent, enrolled retirement plan agent, or enrolled actuary
- Refusing to provide clients with copies of their tax return
- Preparing client returns using off-the-shelf tax software or IRS Free File

Understand that you will only receive acknowledgement of your complaint.

Reminders

- PTINs and enrollment numbers belong to you, not the firm or business. When obtaining either, use a personal email address. One of the biggest issues we see is tax pros being unable to access their online PTIN Account once they no longer have access to the email address assigned by the firm/business.
- RPO will **never send unsolicited** emails requesting your PTIN, or an update to your PTIN information. When in doubt, contact the PTIN Account Information Line – 877-613-PTIN (7846).

Reminders (cont.)

- **Check your online PTIN account regularly. RPO sends messages/correspondence to your secure mailbox. You can also use your online account to:**
  - Track the number of tax returns associated with your PTIN in the calendar year (must have filed a minimum of 50 returns).
  - Track your continuing education credits
  - Update your account information (e.g. mailing addresses, business name, phone numbers, etc.)

IRS2Go Mobile App

IRS.gov/irs2go

IRS2Go is the official mobile app of the IRS

Check your refund status, make a payment, find free tax preparation assistance, sign up for helpful tax tips, and more!

IRS2Go is available in both English and Spanish.

Download IRS2Go for your mobile device

GET IT ON Google Play

Download on the App Store

Available at amazon

IRS2Go offers many features

Connect With the IRS

IRS2Go mobile app

YouTube: IRS videos

X (formerly Twitter): @IRStaxsecurity

Facebook: @IRS

Instagram: @IRSnews

e-News subscriptions

www.irs.gov/socialmedia

Richard Furlong, Jr.

Senior Stakeholder Liaison

267-941-6343

richard.g.furlong@irs.gov