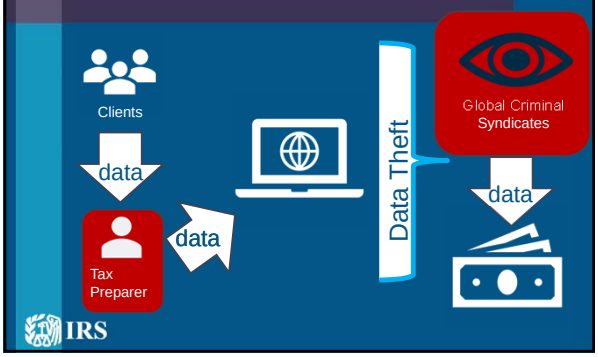
Protect Your Clients; Protect Yourself: Tax Security 101

IRS
Richard Furlong, Jr.
Senior Stakeholder Liaison

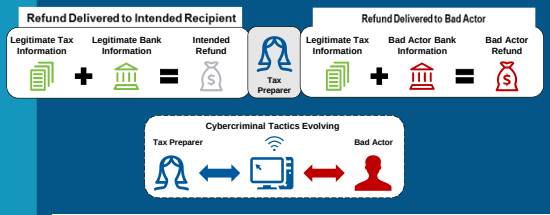
42nd Annual Delaware Federal & State Tax Institutes
December 10, 11, & 13 2018

Tax Security 101



Tax Pro Data Thefts Trending UP

Because of Security Summit safeguards, thieves need legitimate tax information to file fraudulent tax returns.



Thieves also steal EFINs, PTINs and CAF numbers to impersonate tax pros.

IRS

Security Summit Progress – 2015-2017

Because the IRS does a better job of stopping fraudulent returns from entering the processing pipeline, key indicators of identity theft show a dramatic decline.

597K
Number of confirmed IDT tax returns.
Down **57 percent** since 2015.

242K
Number of taxpayers self-reporting as IDT victims.
Down **65 percent** since 2015.

144K
Number of refunds recovered by bank partners.
Down **58 percent** since 2015.

IRS

Overview

- **IRS Publication 4557**
  - **Safeguarding Taxpayer Data**
- **NIST-**
  - **Small Business Information Security: The Fundamentals"**
    - **Identify: Data, People, Equipment "The Printer Breach"**
    - **Protect: Limit Access, Updates, Firewalls, "Lost Passwords and Remote Access Breaches"**
    - **Detect: Anti-Virus, Spyware, "Lost Passwords to Spear Phishing and Malware Breaches"**
    - **Respond: Information Security Plan**
    - **Recover: Backups, "Ransomware Attack"**

IRS

Threats, Vulnerabilities, Likelihood, and Impact

IRS

Identify (Categories)

Access Control

- Identify and control who has access to your business information
- Conduct Background Checks
- Require individual user accounts for each employee
- Create policies and procedures for information security

IRS

Identify
Asset Management / Risk Assessment

- Identify what information your business stores and uses

	Example: Client files	Payroll Data	Employee Files		
Cost of revelation (Confidentiality)	High				
Cost to verify information (Integrity)	High				
Cost of lost access (Availability)	High.				
Cost of lost work	High				
Fines, penalties, customer notification	High				
Other legal costs	High				
Reputation / public Relations costs	High				
Cost to identify and repair problem	High				
Overall Score:	High				

IRS

Identify
Develop an Inventory of IT Related Equipment

- Can a CPA transfer the risk of the data storage to a 3rd party?

	Description (e.g. nickname, make, model, serial number, service ID, other identifying information)	Location	Type of information the product comes in contact with.	Overall Potential Impact
1	Cell phone; Type – Sonic; Version – 9.0 ID – "Police Box"	Mobile T&S Network	Email; Calendar; Customer Contact Information; Photos; Social Media; Locations; Medical Dictionary Application	High
2	Computers			
3	Printers			
4	Wireless Routers			
5	Remote Access			

IRS

Identify (Potential Vulnerabilities)

- **Office printer with wireless capabilities attached to the network.**
- **Unsecured cell phones and IPADs tied into the network.**
- **WIFI Access – Customers**

Change manufacturer default passwords

If you don't do these things, this could happen to you:

https://youtu.be/2ZlZTj5Lh5Q?t=1m13s

IRS

Protect

- Limit employee access to data and information
- Patch your operating systems and applications
- Install and activate software and hardware firewalls on all your business networks
- Secure your wireless access point and networks
- Set up web and email filters
- Use encryption for sensitive business information
- Dispose of old computers and media safely
- Train your employees

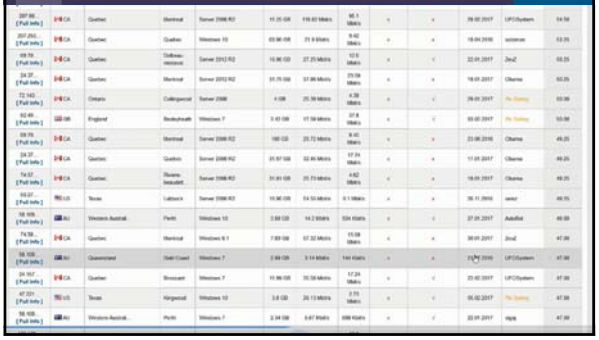
IRS

Protect
Practitioner Breach 2 "Remote Access"

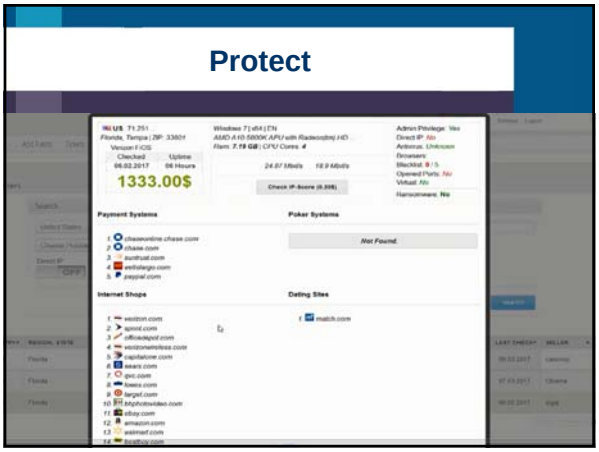
- IT Service Provider on monthly retainer
- December 2016 IT Provider identifies attempted access via Remote Access Program
- January 2018 upgrades Remote Access to VPN
- February 2018 returns rejected
- IT forensics reveal remote access compromise via employees infected home computer in 03/17
- Perpetrator loaded hidden program granting full access and capable of copying and extracting files
- Program concealed using a common file naming convention went undetected from 03/17 to 02/18
- 1/3 of clients ID Theft Victims

IRS

Dark-web site



Protect



Detect

- Install and update anti-virus, -spyware, and other –malware programs
- Maintain and monitor logs
- Passwords should be at least 10 characters

  “Theresnocryinginbaseball2018$!”

- https://www.youtube.com/watch?v=RJJEyGkS9jA

IRS

Protect (Phishing Emails)

From: Posing as Outside Private Sector Entity
Date: Thu, Jun 22, 2017 at 10:54 AM
Subject: Database Error
To: Tax Practitioners

In our database, there is a failure, we need your information about your account.
In addition, we need a photo of the driver's license, send all the data to the letter. Please do it as soon as possible, this will help us to revive the account.

*Company Name *
*EServices Username *
*EServices Password *
*EServices Pin *
CAF number
Answers to a secret question
*EIN Number *
*Business Name *
*Owner/Principal Name *
*Owner/Principal DOB *
*Owner/Principal SSN *
*Prior Years AGI

IRS

Phishing E-mail (Continued)

*From:*SimonandMelisa Willetts [mailto:willettssimonandmelisa@gmail.com]
Sent: Monday, February 20, 2017 6:58 AM
To: Tax Practitioner
Subject: Re: Our 2016 Taxes

My wife and I should have all our 2016 docs in a week or two.

Last year we moved from Wyomind DE -- Mr Pryor was our previous CPA.

Here is our 2015 Tax Documents for your review.
However, we can be on a call Friday 10AM -- OK?

Simon & Melissa Willetts Shared - Tax Documents

<http://rktaxprep.info/customers/Pryordocs2015/pdf/

On Fri, Feb 17, 2017 at 8:45 PM, Tax Practitioner wrote:

Good morning Simon & Melisa,

Yes, I am accepting new clients. Are you in the City area?
Would you like to set up a time to meet?

IRS

Phishing E-mail (Continued)

From: Tax Software Company
Sent: February 13, 2017 12:16 PM
To: Tax Professional
Subject: Access Locked

Dear Customers ,

Access to Tax Software has been suspended due to error(s) in your security details.

Follow the link below to unlock your access

Unlock

Thank you.
© Copyright 2017 Tax Software. All rights reserved.

IRS

Phishing E-mail (Continued)

From: Impersonating a Software Company
To: Tax Practitioner
Sent: 8/10/2016 7:14:26 A.M. Eastern Daylight Time
Subj: Software Update Notification (Do NOT Reply)

Software Company Product Notification System

Dear Client,

Please DO NOT Reply to this e-mail.
All replies to this address will not be received by Software Company.

Please download and install this important update to your computer.

Click Here

Thank you for using XXXXX Software.

-Customer Support.

IRS

Phishing E-mail (Continued)

IRS

Dear User:

Your e-services account is secure. We are doing a one time verification to your e-mail. This will work as a recovery in case your account is compromised. Click or copy the link below to your browser to complete this process.

https://la2.www4.irs.gov/pub/rup_login_1?TYPE=33554433&REALMOID=06-3e42c2f4-1c41-0019-0000-25b0000025b0&GUID=&0000--4d5700004d57%26GUID%3d%26SMAUTHREASON%3d0%26METHOD%3dGET%26SMAGENTNAME%3dIgjzN0Exzjjq7GXjaiQAtum2vjVbftpJfXjCX5EEznNQ6gB2VzGstn8fCh3KSapr%26TARGET%3d--SM-----%2fPORTAL----PROD-%2fCRM-%2fsignon-%2ehtml

If you need any assistance with changing your password, please read the e-services FAQ. On-line assistance is also provided within the Change Password function.

IRS

https://youtu.be/2ZlZTj5Lh5Q?t=38s

Detect
Practitioner Breach 3 “Malware”

- Tax practitioner opens E-Mail with attachment and clicks on attachment.
- IT Forensics reveal hidden program granting access was loaded when the attachment was opened
- Malware and key logger were downloaded on network
- Users on the network logged into various portals which allowed the username and passwords to be accessed.
- Perpetrators were able utilize the username and passwords to gain full access to financial information.

IRS

Respond

Develop a plan for disasters and information security incidents

- The plan should include the following Roles and Responsibilities:
  - Who makes the decision to initiate recovery procedures and contact law enforcement.
  - What to do with your information systems (i.e. shut down/lock computers, move to backup site).
  - Contact IRS and State Tax Authorities.
  - Who to call in case of an incident (i.e. How and when to contact senior executives, emergency personnel, cybersecurity professionals, legal professionals, service providers, or insurance providers).
  - State Notification Laws.

IRS

Respond

IRS

- Tax professionals should contact IRS Stakeholder Liaison when a compromise is detected. The Stakeholder Liaison will refer Information within IRS (i.e. Criminal Investigations, Return Integrity & Compliance Services

http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Stakeholder-Liaison-Local-Contacts-1

State Tax Agencies

- Tax professionals can e-mail the Federation of Tax Administrators to get information on how to report victim information to the appropriate state authorities.

IRS StateAlert@taxadmin.org

Recover

- Make full backups of important business data/information
- 3-2-1 Backup Process (3 Sources, 2 external, 1 offsite)
- Make incremental backups of important business data/information
- Make improvements to processes / procedures / technologies
- Routinely test the backups.

IRS

Recover
Practitioner Breach 4 "Ransomware"

- Delivery of the ransomware came in the form of phishing e-mail to the human resource manager.
- Partner of the firm clicked on the link and ransomware was installed onto the network.
- Ransomware shutdown the system and demanded payment of $1,500 in Bitcoins.
- Perpetrators threatened to sell the PII on the dark web.

IRS

Forensic Results

First Logon Date	Time	User	IP	Country
10/28/2017	4:21:07 AM	tmartin	89.163.148.140	Germany
9/14/2017	12:45:48 PM	ktaylor	212.92.120.238	Netherlands
7/20/2017	6:38:56 PM	jbates	46.166.169.84	Lithuania
7/20/2017	6:39:18 PM	dguertin	46.166.169.84	Lithuania
7/20/2017	6:39:37 PM	creid	46.166.169.84	Lithuania
7/17/2017	11:55:23 PM	myoney	46.166.169.84	Lithuania
7/11/2017	1:05:52 PM	jburns	41.189.161.223	Ghana
7/7/2017	3:10:14 PM	jmiller	188.138.152.105	Moldova

- The source of the remote connections originated from 23 unique countries, including Nigeria, Russia, Moldova, and Egypt.
- The earliest successful unauthorized was made on 7/1/2017 @ 3:10pm. The last unauthorized logon was made on 12/16/2017 @ 5:53pm.

IRS

Cybersecurity Resources

- **Internal Revenue Service (IRS) Publication 4557**
  https://www.irs.gov/pub/irs-pdf/p4557.pdf
- IRS Resources for Tax Professionals - **Protect Your Clients; Protect Yourself**
  https://www.irs.gov/individuals/protect-your-clients-protect-yourself
- **Federal Trade Commission -** FTC Start with Security
  https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security
- **National Institute of Standards and Technology (NIST) -** Small Business Information Security: *The Fundamentals*
  http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

IRS

New Twist to Old Scam

IR-2018-17, Feb. 2, 2018

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 has already identified a new scam that began with cybercriminals stealing data from several tax practitioners' computers and filing fraudulent tax returns.

In a new twist, the fraudulent returns in a few cases used the taxpayers' real bank accounts for the deposit. A woman posing as a debt 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.

IRS

Cybercriminal Tactics

Spear Phishing emails

- 91% data thefts start with a phishing email
- From "Trusted" source
- Urgency – "Act Now"
- Contains embedded link or attachment
- Intent – steal passwords or download malware

Remote Access Takeover

- Thieves gain control of office networks
- Email scams
- Malware
- Hacking unprotected devices
- All wireless devices are vulnerable
- Reset factory passwords

Ransomware

- Phishing email, or
- Failure to update software
- Thieves encrypt all data on the computer
- Demand a ransom in return for a "key" to unlock encrypted data
- If paid, unlikely to provide the key

IRS

FTC & Gramm-Leach-Bliley Act

IRS

FTC "Safeguards Rule"

- Designate one or more employees to coordinate the information security program
- Identify and assess the risks to consumer information in each relevant area of company operations
- Design, implement a safeguards program
- Require service providers to maintain safeguards
- Adjust program as needed

IRS

Pub 4557 – Safeguards Checklist

ONGOING	DONE	N/A	Employee Management and Training
☐	☐	☐	The success of your information security plan depends largely on the employees who implement it. Consider these steps:
☐	☐	☐	Check references or doing background checks before hiring employees who will have access to customer information.
☐	☐	☐	Ask every new employee to sign an agreement to follow your company's confidentiality and security standards for handling customer information.

IRS

Basic Security Steps

- Recognize and avoid phishing emails.
- Create data security plan using Publication 4557, Safeguarding Taxpayer Data, and Small Business information Security – The Fundamentals.
- Review internal controls:
  - Install security software
  - Create strong passwords, 8 characters or more
  - Encrypt sensitive files

IRS

Basic Security Steps

- Back up sensitive data
- Wipe clean or destroy old hard drives
- Limit access to taxpayer data
- Check IRS e-Services weekly for EFIN counts

- Report Data Thefts immediately to the IRS Stakeholder Liaisons
- Stay connected to the IRS: Subscribe to e-News for Tax Professionals, QuickAlerts and social media

IRS

Signs of Data Theft in Your Office

- 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;
- Clients receive tax transcripts that they did not request;
- Clients who created an IRS online services account receive an IRS notice that their account was accessed or disabled

IRS

Signs of Data Theft in Your Office

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

IRS

How Tax Pros Report Data Theft

- Contact IRS and law enforcement
  - IRS stakeholder liaisons are your points of contact
  - Search "stakeholder liaisons" on IRS.gov
- Contact state tax agencies/attorneys general
  - Email Federation of Tax Administrators for stat agency contacts at StateAlert@taxadmin.org
- Contact Experts
  - Security expert and/or insurance company
- Review "Data Theft Information for Tax Professionals" at IRS.gov/identitytheft

IRS

Obligation to Cooperate – Pub 3112

"Safeguarding of IRS e-file from fraud and abuse is the shared responsibility of the IRS and Authorized IRS e-file Providers. Providers must be diligent in recognizing fraud and abuse, reporting it to the IRS, and preventing it when possible. Providers must also cooperate with the IRS' investigations by making available to the IRS upon request, information and documents related to returns with potential fraud or abuse."

IRS

Steps to protect client data

- Review current security measures
- Create a security plan
  - Use top-notch software security
  - Educate all employees
  - Use strong passwords
  - Secure Wi-Fi
  - Encrypt PII emails
  - Backup files

IRS

Taxpayer Protection Program

TPP Letters	Action	File a F14039
4883C	Call the IRS	No
5747C	Visit IRS office	No
5071C	Use online verification	No
None	Unable to e-file return due to duplicate SSN	Yes

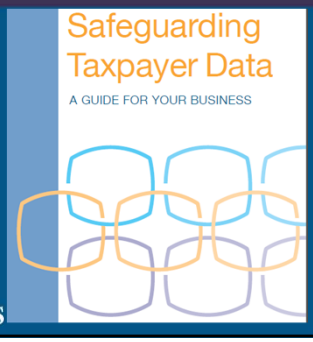
IRS

Security Resources for Tax Pros

- Publication 4557, Safeguarding Taxpayer Data
- Publication 5293, Data Security Resource Guide for Tax Professionals (NEW)
- www.IRS.gov/ProtectYourClients
- www.IRS.gov/IdentityTheft
  - —Individuals
  - —Tax Pros
  - —Businesses

IRS

Publication 4557



Publication 4557

- Revised and Updated
- How-to security
- Signs of IDT
- Recovery and respond
- Comply with FTC rules

IRS

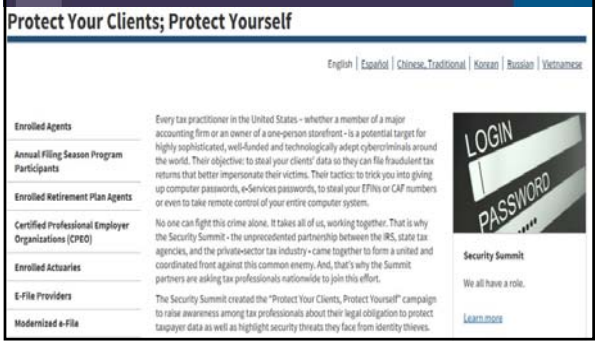
Publication 5293

Publication 5293

- Compiles IRS.gov resources
- Bookmarks security pages
- Fast reference for security & reporting tips
- Share with all employees

IRS

Search on IRS.gov: "Protect Your Clients; Protect Yourself"



e-Services two-factor authentication

- Developed Secure Access Authentication
  - —Two-step authentication for returning user
    - Credentials (username/password)
    - Security code text
  - —Meets OMB and NIST standards
  - —Protects Get Transcript Online and IP PIN tools
  - —Risk assessment conducted on other IRS.gov tools

IRS

Monitor Your EFIN, PTIN and CAF Numbers

IRS

Stolen EFINs, PTINs and CAFs

- Thieves impersonate tax pros to:
  - File fraudulent returns
  - Submit Power of Attorney forms
  - Call Practitioner Priority Service line
  - Attempt to access client accounts
  - Attempt to access e-Services
- IRS responses include:
  - 2-factor authentication for e-Services accounts
  - Authorization requirements for PPS callers
  - Redacted tax transcripts

IRS

Maintain Your EFIN Application

- Only the IRS can issue EFINs
- Review periodically for accuracy and updates
- Update change in business operations within 30 days
  - Changes in address, phone numbers or personnel
  - Add or remove authorized users (responsible officials, principal consent, delegated users, etc.)
- Know when a new EFIN is needed
  - New ownership of a firm (EFIN not transferable)
  - New location that transmits e-File returns

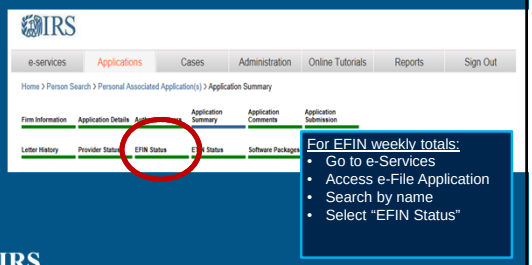
IRS

Protect your EFIN

- IRS reviewing improvements to EFIN safeguards
  - —Stepped up efforts to expel EFIN abusers;
  - —Increased on-site visits as part of monitoring process
- EFIN holders should review return numbers during filing season
  - —e-Services Account updated weekly
  - —Excessive numbers can be reported to e-Help Desk

IRS

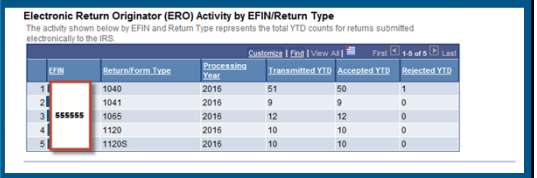
Monitor Your EFIN



For EFIN weekly totals:
- Go to e-Services
- Access e-File Application
- Search by name
- Select "EFIN Status"

IRS

Report Suspected EFIN Abuse



- Too many returns filed with your EFIN? Contact e-Help Desk (866) 255-0654

IRS

Monitor Your PTIN

- Monitor "Returns Filed per PTIN"
- Information available via online PTIN system for tax preparers who meet both of the following criteria:
  - Have a professional credential or are an Annual Filing Season Program participant, **and**
  - Have at least 50 Form 1040 series tax returns processed in the current year

IRS

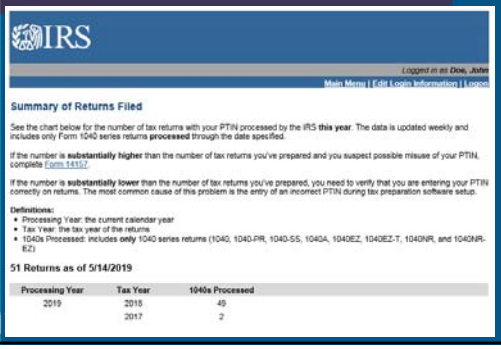
How to Access PTIN Information

To access "Returns Filed Per PTIN" information, follow these steps:

1. Log into your PTIN account
2. From the Main Menu, find "Additional Activities"
3. Under Additional Activities, select "Summary of Returns Fied."

IRS

Summary of Returns Filed Chart


IRS

Logged in as Doe, John

Main Menu | Edit Login Information | Logout

Summary of Returns Filed

See the chart below for the number of tax returns with your PTIN processed by the IRS **this year**. The data is updated weekly and includes only Form 1040 series returns **processed** through the date specified.

If the number is **substantially higher** than the number of tax returns you've prepared and you suspect possible misuse of your PTIN, complete Form 14157.

If the number is **substantially lower** than the number of tax returns you've prepared, you need to verify that you are entering your PTIN correctly on returns. The most common cause of this problem is the entry of an incorrect PTIN during tax preparation software setup.

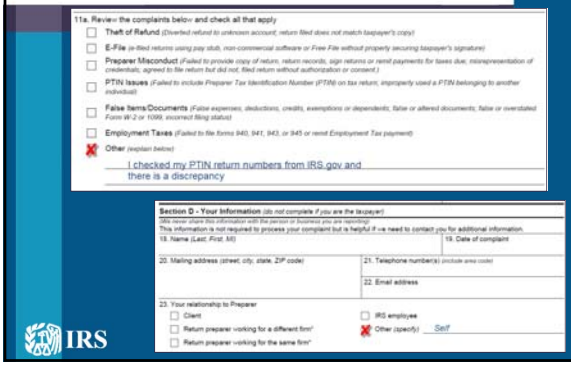
Definitions:

- Processing Year: the current calendar year
- Tax Year: the tax year of the returns
- 1040s Processed: includes **only** 1040 series returns (1040, 1040-PR, 1040-SS, 1040A, 1040EZ, 1040EZ-T, 1040NR, and 1040NR-EZ)

51 Returns as of 5/14/2019

Processing Year	Tax Year	1040s Processed
2019	2018	49
	2017	2

Report Misuse of your PTIN


11a. Review the complaints below and check all that apply

- [ ] Theft of Refund (Diverted refund to unknown account; return filed does not match taxpayer's copy)
- [ ] E-File (e-filed returns using pay stub, non-commercial software or Free File without properly securing taxpayer's signature)
- [ ] Preparer Misconduct (Failed to provide copy of return; return records; sign returns or remit payments for taxes due; misrepresentation of credentials; agreed to file return but did not; filed return without authorization or consent.)
- [ ] PTIN Issues (Failed to include Preparer Tax Identification Number (PTIN) on tax return; improperly used a PTIN belonging to another individual)
- [ ] False Items/Documents (False expenses, deductions, credits, exemptions or dependents; false or altered documents; false or overstated Form W-2 or 1099; incorrect filing status)
- [ ] Employment Taxes (Failed to file forms 940, 941, 943, or 945 or remit Employment Tax payment)
- [x] Other (explain below)

I checked my PTIN return numbers from IRS.gov and there is a discrepancy

Section D - Your Information (do not complete if you are the taxpayer)

We never share this information with the person or business you are reporting!
This information is not required to process your complaint but is helpful if we need to contact you for additional information.

18. Name (Last, First, MI) | 19. Date of complaint

20. Mailing address (street, city, state, ZIP code) | 21. Telephone number(s) (include area code) | 22. Email address

23. Your relationship to Preparer

- [ ] Client
- [ ] Return preparer working for a different firm*
- [ ] Return preparer working for the same firm*
- [ ] IRS employee
- [x] Other (specify): Self

IRS

Maintain Your POA Files

- A CAF number is assigned the first time you file a third-party authorization with IRS.
- Review your Power of Attorney submissions annually
- Withdraw your POA for clients you no longer represent by mailing or faxing the existing POA to the IRS using the “Where to File” chart. Write “Withdraw” at the top.

IRS

Monitor Your CAF Number

- Using stolen CAF numbers to try to obtain tax transcripts is the latest ID theft trend.
- Receiving unexpected tax transcripts is a sign of identity theft.
- Contact the IRS if there is suspected abuse of your CAF number.
- Review Publication 4557, Safeguarding Taxpayer Data, for additional security steps

IRS

Practitioner Priority Service (PPS) 866-860-4259

- PPS voice options:
  - Option 1 - Tax Law questions
  - Option 2 - Individual Accounts not in collection or examination status
  - Option 3 - Business Accounts not in collection or examination status
  - Option 4 - Automated Collection System (ACS) status
  - Option 5 - Automated Under Reporter (AUR) status
  - Option 6 - Correspondence Examination

IRS

Contact Information

Richard Furlong, Jr.
Senior Stakeholder Liaison
267-941-6343
richard.g.furlong@irs.gov

IRS