August 16, 2023
Pacific Northwest Action Wednesday IMRS Call
Virtual Meeting via MS Teams
Time: 10:00 am –11:00 am (PDT)

Attendees:

Internal Revenue Service

- John Blakeman, Stakeholder Liaison
- Mercean Lam, Stakeholder Liaison
- Lisa Novack, Stakeholder Liaison
- David Higgins, Collection [on Detail to Stakeholder Liaison]
- Lelah Martinez, Stakeholder Liaison
- Kristen Hoiby, Stakeholder Liaison

Practitioner Representatives

- Terry Bakker, OAIA
- Laurie Brock, TAP Oregon, prev.
- Steve Stauss, NM
- Robin Smith, WSTC
- Steven Fox-Middleton, WA
- Judy K Hanson, WSTC President
- Barb Haluschak, WSTC
- Lisa Rogers, AKSCPA
- Ami Oppe, AKSCPA
- Elliot Gidan, CO
- Kate Grubb, WSSEA
- Larry Hess, NMSCPA
- James Adelman, NAEA, OSEA
- Doug Henne, OSCPA
- Barbara Culver, WSSEA
- Dale Marino, OATC
- Ellen Briscoe, NMSEA, NATP
- Steven Hall
- Anne Rothrock, NM
- Mark Neumeister, OK
- Michael Davidson, ORSEA
- Donna Patterson, TAP Washington
- Edwin del Carpio, WA
- Vera Likhonin, STA, WA
- Paula Moore, AK Bar
- Robin Harris, OK
- Sarah Northcutt, OSCPA
- Sarah Lora, Lewis & Clark LITC
- Cynthia Polley, WA

Meeting Summary

Data Security for Tax Professionals:

Just in case you have not heard the news… as of June 9, 2023, the FTC Standards for Safeguarding Customer Information rule, better known as the Safeguards Rule (which is part of the Gramm-Leach-Bliley Act) has now entered the enforcement stage.

The Rule requires financial institutions to develop, deploy and maintain a comprehensive security program to keep their customer financial data safe. Financial institutions are not just banks under the FTC's eyes. Tax and accounting professionals are considered financial institutions regardless of size. This also includes mortgage brokers, real estate appraisers, universities, nonbank lenders, and check cashing businesses.

The good news is that if you have already been complying with IRS Publication 4557, Safeguarding Taxpayer Data, you will already be in good shape and may only need to add a few additional security measures to comply with the FTC Safeguards Rule.

The concern will be for firms who have been attesting that they have a Written Information Security Plan (WISP) in place for their PTIN renewal, but really don't.

Pub 4557, Safeguarding Taxpayer Data, and the Safeguards Rule:

Pub 4557

It is important to understand how Pub 4557 and the Safeguards Rule work together, IRS Publication 4557 sits "under" or "within" the FTC Safeguards Rule. All firms who provide tax prep services for their clients are subject to BOTH Pub 4557 and the Safeguards Rule, because providing paid tax preparation services is called out specifically on the FTC website and IRS Publication 4557.

Under Both

Firms must designate a person to be in charge to make sure that security policies are adhered to. The designate will assess overall risk, and then design policies to ensure that all Personally Identifiable Information (PII) and Customer Information is encrypted, transmitted, and stored safely. Access would be limited to only those who need it, and background checks being required before hiring employees or contractors. Security software must be used, all hardware is encrypted and inventoried, network protections are put in place, strong password policies adhered to, and Multi-Factor Authentication used. A WISP, or Written Information Security Plan, is created to document that the firm is following all recommended security requirements and has the necessary policies and procedures in place to keep all clients' data safe. Annually, staff are trained, safeguards are tested and the WISP is reviewed for updates.

Just FTC

For firms with 5,000 or more combined current and past clients on their data banks that provide client accounting services (CAS) (Financial Planning) or Payroll Services, FTC mandates that these companies also adhere to the Safeguards Rule.

Also just within the FTC requirements is choosing a QUALIFIED individual to assess the security risk in the firm's operations, create a Written Risk Assessment, and then create policies and procedures to mitigate the risks. These policies from the firm's WISP or Written Information Security Plan will be used to ensure that all staff are trained to prevent and spot security risks. Additionally, that person must report annually to the firm's Board of Directors.

If you are overwhelmed or have a smaller firm and don't have a qualified IT person working in-house or under contract, you should consider engaging a Managed Service Provider (MSP) to manage the firm's overall data and network security infrastructure and to help in creating the policies required and rolling them out to your staff.

Publication 5708 – Creating a Written Information Security Plan for Your Tax and Accounting Practice

Creating a WISP

If you are a do-it-yourself-er, the bare essentials of a Written Information Security Plan are outlined on page 4 of Pub 5708, with links for more details within each section.

There is also a fill-in-the blank sample WISP template on pages 5-12

Additional Considerations – On pages 13-16 it gives you more explanation on how to:

- Define the WISP objectives, purpose and scope
- Identify responsible individuals
- Assess Risks
- Inventory Hardware (template on page 24)
- Document Safety Measures – Like how to set up policy for remote workers
- Draft an Implementation Clause stating when security measures are started and how they are compliant with the Gramm Leachy Bill Act and FTC
- Include certain attachments such as the Records Retention Policy

Best Practices:

- Going over written security rules of conduct and having your employees sign it before each filing season and using articles from the Ouch! Newsletter from SANS.ORG for security topics at staff meetings.
- Have a list of who can access PII and what information they have access to

Some additional Resources:

In addition to Pub 4557 and 5708, here are a couple of additional resources…firstly, to the Federal Trade Commission website: Federal Trade Commission | Protecting America's Consumers (ftc.gov) and here is a copy of the FTC Data Breach Response Guide:

FTC DB Response Guide for Business

The Data Breach Response Guide is AMAZING! It spells everything that you need to do, from taking your systems down to a sample client letter. IRS mentions it in our Publication 5708 to read before starting to draft your WISP.

IPPIN Program:

What else can we do to thwart identity thieves from filing fraudulent tax returns? We can all help promote the IPPIN program!

Some folks view the IPPIN program as a positive thing and already actively promote it, but some are not so sure it's a good thing…or at least it's not *that* good yet.

We have heard a lot of feedback by this time on the IPPIN Program, both positive and negative, but The biggest reason that we hear that practitioners do not want to promote it is because that their clients lose them. Yes, this is true…clients lose 1099s and W-2s also…and other stuff…we've all got stories.

An IPPIN is often retrievable: Retrieve Your IP PIN | Internal Revenue Service (irs.gov)

But if they can not retrieve it, you will have to print out their return and have them sign, date and mail it to the IRS. And, of course, you might be thinking, 'I don't want my client's returns to end up in a stack of paper…' but let's look at the current statistics. According to our Mission-Critical Function page as of August 16, 2023, on the backlogs:

- Processing for paper 1040's without errors is now just taking 21 days, which is where this return would end up

  versus

- Taking 430 days if your client's information gets fraudulently filed by an ID thief.

Another reason we hear is that the IPPIN is just too hard to get…some folks just can't seem to get past the identity verification process. Specifically, they can't seem to be able to get the ID.me credential. Please remember, there are other ways to get the IPPIN, and you can get info on that here at this link: Get An Identity Protection

PIN | Internal Revenue Service (irs.gov). For example, Form 15227 for people with certain AGI levels, and of course at a Taxpayer Assistance Center [TAC]. Taxpayer Advocate can also assist with the process for people who are disabled/mobility challenged and can't get to the TAC.

And then there's the 'I just don't want to sign up for it…or promote it…etc…'. Which is also human nature, but consider this…IPPIN is a valid tool for keeping fraudulent tax returns from being filed…if you do get breached, and if your client[s] have fraudulent tax returns filed and there was a way to avoid that…a way that you knew about, but didn't say…that might not look so hot to some people…

Currently trending in the myriad of ways systems are hacked/breached are:

- Phishing texts impersonating the IRS
- Software [fraudulent] companies letting practitioners know that they have been breached [that's a tough one…remember to call your software provider, and not any number in the email!]
- Insider threats (physical theft and employee retaliation)
- Cloud-based platforms being accessed
- Impersonators (like Geek Squad, MicroSoft, Microsoft Defender, web developers, IRS and credit card companies)
- Live screenshare

As a reminder, if you have not heard about the IRS impersonation mail scam, do a search for IRS News Release IR-2023-123 : IRS, Security Summit partners warn taxpayers of new scam; unusual delivery service mailing tries to trick people into sending photos, bank account information | Internal Revenue Service .

This new release speaks to a new IRS impersonating mailing scam that tries to mislead people into believing that they are owed a refund. It asks for things like copies of their drivers licenses along with other PII. The grammar is off and it mentions getting a property claim instead of a tax refund. Since this is a scam impersonating the IRS, these incidents should be reported to TIGTA.

IRS Ends Unannounced RO Visits:

As part of a larger transformation effort, the Internal Revenue Service today announced a major policy change that will end most unannounced visits to taxpayers by agency revenue officers to reduce public confusion and enhance overall safety measures for taxpayers and employees.

The change reverses a decades-long practice by IRS revenue officers, the unarmed agency employees whose duties include visiting households and businesses to help taxpayers resolve their account balances by collecting unpaid taxes and unfiled tax returns. Effective immediately, unannounced visits will end except in a few unique circumstances and will be replaced with mailed letters to schedule meetings.

IRS Commissioner Danny Werfel announced the change as part of a larger effort to transform IRS operations following passage of the Inflation Reduction Act last year and the creation of the new IRS Strategic Operating Plan in April.

Taxpayer Assistance Centers to reopen:

35 TACs have reopened or been added thanks to the IRA funding…relevant to us PNWAW folks, this means that we'll see TACS again at Bend, OR; Bellingham, WA; Colorado Springs, CO; Grand Junction, CO; Santa Fe, NM; and Glendale, AZ

Issues, Questions and Concerns:

Update: we have formally submitted the issue regarding IRS handling of Form 56.

Concern: We had a few questions on IPPINS today, one with a person who could not find their IPPIN and others with issues getting ID.me credential…Please see the section on IPPINs above for links to information and assistance.

Comment: One practitioner commented that while they don't promote the IPPIN program actively, they do have clients who have signed up and the last few have received an IPPIN in about half an hour, so there has been real improvement to the level of service on the phones.

Q: Is there an option to 'opt out' of the IPPIN program?

A: Currently there is no option for opting out of the program…it is under consideration, but nothing definitive.

Q: I see the IRS is expanding free file. When will this be rolled out more extensively? What are the restrictions for use? Does it still rely on providers that re-direct to paid file? What can we expect in the future on this front?

A: We will look into this and report back at the next meeting.

Q: Seems the Tax Pro Online Account was supposed to get some new functionality in the way of linking and viewing POAs, but we are not seeing that it has happened yet? Any news?

A: It could be that the changes have not *altogether* taken place yet. Sometimes there's a few days delay…and one preparer did comment that one needs a PIN for complete functionality and the process takes a few weeks…

Q: ID.me is still really hard to get…next to impossible for some people. We have a client with some physical challenges that make it hard to get past the ID.me process.

A: We are hearing this from time to time regarding the folks with real physical or mental challenges not being able to work with ID.me. TAS has offered to help in these situations where the person may have issues that make ID.me unavailable for

all practical purposes…or at least to do it on their own. So if the client is in a memory care facility, or other debilitating situation, TAS can help facilitate communication.

Q: How would we report these abusive ERC scheme promoters if we encounter them?

A: Here is the web page on IRS.gov with the information on reporting abusive scams: Abusive Tax Schemes and Abusive Tax Return Preparers - IRS Lead Development Center | Internal Revenue Service

We have an excellent web page on IRS.gov that speaks to the ERC, including signs of scams, and the link to the FAQ page as well: Employee Retention Credit | Internal Revenue Service (irs.gov)

Next Scheduled Meeting, Wednesday September 20, 2023