August 21, 2024
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
- Lelah Martinez, Stakeholder Liaison
- Mercean Lam, Stakeholder Liaison
- Michael Smith, Stakeholder Liaison
- David Higgins, Stakeholder Liaison
- Kristen Hoiby, Stakeholder Liaison
- Melissa Chapman, Taxpayer Advocate Service
- John Little, Taxpayer Advocate Service
- Jacqueline Schmitt, Taxpayer Advocate Service
- Sarah DeBurle, Taxpayer Advocate Service
- Tonia Large, Taxpayer Advocate Service

Practitioner Representatives

- Ami Oppe, AKSCPA
- Terry Bakker, OAIA
- Edwin del Carpio, WA
- Kristen Keats, OSCPA
- Robin Smith, WSTC
- Harriet Strothers, OSCPA
- Kate Grubb, WSSEA
- Teresa Moore, EA WY
- Jeremy Saladino, WAATP
- Larry Hess, NMSCPA
- Vera Likhonin, WA
- James Adelman, OK SEA
- Jeffrey Quatrone, AZ
- Mark Neumeister, OK
- Dale Marino, OSTC
- Eliott Gidan, CO
- Judy Hanson, WSTC President
- Robin Harris, OK
- Steven Stauss, NM
- Barbara Culver, WSSEA
- John Hawkins, OSCPA
- Stephan King, ASCPA
- Lisa Rogers, AKSCPA
- Melissa Burr, OSCPA
- Gail Baudendistel, WA
- Robin Harris, OK

Meeting Summary

Mercean Lam, Senior Stakeholder Liaison

Form 1099-DA draft form:

The Internal Revenue Service has posted an early draft of the updated Form 1099-DA, which is the form for brokers to report certain sale and exchange transactions of digital assets that take place beginning in calendar year 2025. Generally, these forms will be sent separately to taxpayers and the IRS in early 2026.

The new draft of Form 1099-DA, Digital Asset Proceeds From Broker Transactions **PDF**, reflects the final regulations for **custodial** broker reporting and includes the transitional relief described in Notice 2024-56, Notice 2024-57 and Revenue Procedure 2024-28.

Interested parties can provide the IRS with comments about the draft at the forms and publications comments page on IRS.gov.

As part of the process that will lead to a final version of the form, the IRS posted the new draft of Form 1099-DA to IRS.gov along with the instructions for the recipients of the form. The IRS expects to post the draft instructions for filers soon. Once the draft filer instructions have been posted, a notice will be published in the Federal Register to allow for a 30-day comment period.

Michael Smith, Stakeholder Liaison

ERC Voluntary Disclosure Program is back:

Good news, folks! The Voluntary Disclosure Program is back! The Internal Revenue Service urges businesses that have received Employee Retention Credit payments or still have pending claims to recheck the eligibility requirements and consider the second Employee Retention Credit (ERC) Voluntary Disclosure Program (VDP) to resolve possible incorrect claims without penalties or interest. Businesses are still able to withdraw claims that have not been paid.

The second ERC-Voluntary Disclosure Program will run through Nov. 22, 2024, and allow businesses to correct improper payments at a 15% discount and avoid future audits, penalties and interest. There are some differences between this version and the first round of ERC VDP, so careful review of the rules for 'Round 2' is recommended.

Once the employer has applied to the VDP and submitted their Form 15434, an IRS employee will contact them to go over the application and answer any questions. If the IRS approves the employer's application, they will mail the employer a closing agreement. The employer must then repay 85% of the ERC they received, either online or by phone, using the Electronic Federal Tax Payment System (EFTPS). EFTPS is the Treasury Department system that most businesses already use to pay various federal tax obligations.

Of course, lots more details are in the news release, so please give it a gander: IRS provides details of second Employee Retention Credit Voluntary Disclosure Program; program for improper claims open through Nov. 22 | Internal Revenue Service

David Higgins, Stakeholder Liaison

Security Summit still in swing!

Just this past week, as part of a special eight-part series, with tips being sent each week, the IRS and Summit partners highlighted the newly updated Publication 5708, Creating a Written Information Security Plan for your Tax & Accounting Practice **PDF**. This Written Information Security Plan, or WISP, is a 28-page template designed to help tax pros, particularly smaller practices, create a plan for their office.

The WISP has been updated and expanded to make data security planning easier. The new WISP, the result of a year-long effort, is an easy-to-understand document developed by and for tax and industry professionals to keep customer and business information safe and secure. Tax pros are required to have a security plan under federal law.

The new version of the WISP includes several new information updates since the first version came out. This includes highlighting best practices for implementing multi-factor authentication for any individual accessing any information system, unless their qualified individual has approved in writing the use of reasonably equivalent or more secure access controls.

In addition, tax pros now need to report a security event affecting 500 or more people to the Federal Trade Commission (FTC) as soon as possible, but no later than 30 days from the date of discovery. This is in addition to reporting the incident to an IRS Stakeholder Liaison and state tax authorities.

This week the IRS and Security Summit Partners outlined the 'Security Six' measures. The "Security Six" protections offer a relatively simple but important starting point for tax pros to protect their offices, computers and data as well as their clients. These best practices include using anti-virus software, firewalls, multi-factor authentication, backup software or services, encrypted drives and virtual private networks or VPNs.

Please see the news release at the following link: IRS, Security Summit highlight "Security Six" and key steps for tax pros to protect themselves | Internal Revenue Service

Lelah Martinez, Stakeholder Liaison

Disaster Tax Relief Information on IRS.gov:

Wildfire season is upon us in the Western U.S. right now, but each season brings its own set of natural disasters any more, it seems. If you need to find the current disaster declaration and news for your state, or for historical events as well [which can be vital in preparing some returns], check out the 'Tax relief in disaster

situations' web page: Tax relief in disaster situations | Internal Revenue Service (irs.gov)

There are typically two types of assistance in the declarations we see. The first and most common is 'Public' assistance', which by and large is for assisting state and local governments in their cleanup and debris removal activities. The other type is Individual Assistance, and when that comes into play, so do the disaster tax relief measures. For additional resources relating to disaster tax relief, please see the document below courtesy of our own Lelah Martinez:

IRS Resources - Disaster Assistance.dc

Sarah DeBurle and Tonia Large, Taxpayer Advocate Service

Sarah will be retiring at the end of this month, and Tonia will be the Acting Local Taxpayer Advocate for Washington state. We wish you all the very best in retirement, Sarah…you are such a fine person, and it's been so good to work with you…and best of luck and skill, Tonia! We welcome you with open arms, and we are so glad you are here.

John Blakeman, Stakeholder Liaison

Collector Issues, IMRS and other updates:

Please remember to send your SL any feedback you may have on interactions you have with the following IRS applications and programs:

- IRIS
- Document Upload Tool
- Resumption of Collection Notices
- Digital Assets [cryptocurrency and related issues]
- Inflation Reduction Act
    - Clean energy credits
    - IRS modernization efforts
- Direct File
- American Rescue Plan Act of 2021 [for example, 1099K]

So really, what we are asking is that when you encounter these things, or when you are working with them, please take the time to let us know how your experience was. I know it's hard to remember when we are in the thick of things, but it really goes a long way to helping us improve your experience with us.

Questions and Answers!

Q: We have been getting notices for late file/late pay but the returns were filed timely…the amounts are relatively small in the notices. It seems that the processors are not entering the post mark date and rather the received date?

A: This issue seems to come up every so often, and we will let our IMRS group know it is happening again.

Q: Is it possible to get a comprehensive list of the Service Center/Campus addresses? They are hard to find on IRS.gov.

A: An excellent suggestion…we will put this suggestion forward.

Q: We did not file for very many ERC claims unless we were pretty sure that they qualified. We got one quarter denial on a client we were sure they qualified. The notice said that there was no disaster declaration and the client did not have a large enough decrease in business. We were not required to send quarterly income statements so how did they determine they did not qualify? I do not know what to appeal, or if we should.

A: This is from the Employee Retention Credit page on IRS.gov:

If the IRS disallowed your ERC claim and you disagree, you may request an administrative appeal. You may also file suit in a U.S. District Court or the U.S. Court of Federal Claims. You can submit additional documentation for us to consider when you request an administrative appeal, and we'll consider that information before sending your case to Appeals.

Q: Without knowing why the claim was denied, how do we appeal?

A: Here is an excerpt from the FAQ on in IRS.gov:

Taxpayers may be wondering what a notice of claim disallowance is and what to do next. Here's a quick explanation of the significance of these notices, and how taxpayers can respond. The notice of claim disallowance is a legal notice that the IRS is **not allowing the credit or refund claimed**. A letter 105C is a notice of a full disallowance, and a 106C is a notice of a partial disallowance. If taxpayers don't agree with the IRS's denial of the claim – regardless of which letter the taxpayer received – they can seek review by petitioning the IRS's Independent Office of Appeals (Appeals).

Q: Where should we be using Multi-Factor Authentication [MFA]? Is there any way we could get a list of where we should apply MFA?

A: There was an excellent discussion on this…for sure it should be on your tax software…ANYONE accessing your tax software should need to use MFA to get into the system, but there are other recommended areas…like signing into the business

email account. Below is some helpful information from Pub 4557, Safeguarding Taxpayer Data, as well as the Safeguards rule from the FTC website.

Here are some excerpts from Publication 4557: Safeguarding Taxpayer Data (https://www.irs.gov/pub/irs-pdf/p4557.pdf):

According to the FTC, the required information security plan must be appropriate to the company's size and complexity, the nature and scope of its activities and the sensitivity of the customer information it handles. As part of its plan, each company must:

- implement Multi-factor Authentication: Implement for anyone accessing customer information on your system. The FTC Safeguards Rule requires at least two of these following authentication factors: a knowledge factor (for example a password), a possession factor (for example, a token), and an inherence factor (for example biometric information). This is required for all companies regardless of size.

Page 6
Do not overlook a critical step to protecting accounts: Multi-factor authentication. This simple feature can protect your accounts even if your username and password are stolen. Tax software products for both taxpayers and tax professionals now offer multi-factor authentication. Use the most secure option available, not only for your tax software, but other products such as email accounts and storage provider accounts. An example of multi-factor authentication: you must enter your credentials (username and password) plus a security code sent as a text to your mobile phone before you can access an account.

Multi-factor Authentication (definition, page 18)
A security system that requires returning users to enter more than just credentials (username and password) to access an account or device, such as two-factor or three-factor authentication. Example: e-Services is protected by IRS Secure Access, a two-factor authentication process that requires returning users to enter their credentials and a security code sent as text to a mobile phone. Tax professionals should always use the highest multifactor authentication available.

Here's some excerpts from the Safeguards Rule on multi-factor authentication: eCFR :: 16 CFR Part 314 -- Standards for Safeguarding Customer Information

§ 314.2 Definitions.

(j) ***Information system*** means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing customer information or connected to a system containing customer information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains customer information or that is connected to a system that contains customer information.

(k) ***Multi-factor authentication*** means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password;
(2) Possession factors, such as a token; or
(3) Inherence factors, such as biometric characteristics.

§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(5) Implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls

COMMENT: It would be very helpful to have some information on the 'workflow' of the Document Upload Tool. Currently it doesn't really give any feedback as to whether anything has been done with the documents, nor does it let us know that the right person received them. Where do the documents go?

Response: We will continue to press for more clarification on the DUT and its functionality. We always recommend that if the document has a QR code that you use it when uploading to the DUT.

Next Scheduled Meeting; Wednesday September 18th.