December 14, 2022

CPA Continuing Education Society of Pennsylvania

"IRS Updates"

Topics:

1) Tax Law Changes for 2022

2) Fundamentals and Tax Treatment of Digital Assets & Virtual Currency

3) IRS Updates

Presenter:

Richard G. Furlong, Jr.
Senior Stakeholder Liaison
Stakeholder Liaison
IRS Communications & Liaison Division
267-941-6343
Richard.G.Furlong@irs.gov

Form **1040** Department of the Treasury—Internal Revenue Service **U.S. Individual Income Tax Return** **2022** OMB No. 1545-0074 IRS Use Only—Do not write or staple in this space.

Filing Status Check only one box. ☐ Single ☐ Married filing jointly ☐ Married filing separately (MFS) ☐ Head of household (HOH) ☐ Qualifying surviving spouse (QSS)

If you checked the MFS box, enter the name of your spouse. If you checked the HOH or QSS box, enter the child's name if the qualifying person is a child but not your dependent:

Your first name and middle initial	Last name	**Your social security number**
If joint return, spouse's first name and middle initial	Last name	**Spouse's social security number**
Home address (number and street). If you have a P.O. box, see instructions.	Apt. no.	**Presidential Election Campaign** Check here if you, or your spouse if filing jointly, want $3 to go to this fund. Checking a box below will not change your tax or refund. ☐ **You** ☐ **Spouse**
City, town, or post office. If you have a foreign address, also complete spaces below.	State / ZIP code	
Foreign country name / Foreign province/state/county / Foreign postal code		

Digital Assets At any time during 2022, did you: (a) receive (as a reward, award, or payment for property or services); or (b) sell, exchange, gift, or otherwise dispose of a digital asset (or a financial interest in a digital asset)? (See instructions.) ☐ **Yes** ☐ **No**

Standard Deduction **Someone can claim:** ☐ You as a dependent ☐ Your spouse as a dependent ☐ Spouse itemizes on a separate return or you were a dual-status alien

Age/Blindness **You:** ☐ Were born before January 2, 1958 ☐ Are blind **Spouse:** ☐ Was born before January 2, 1958 ☐ Is blind

Dependents (see instructions): If more than four dependents, see instructions and check here . . ☐

(1) First name Last name	**(2)** Social security number	**(3)** Relationship to you	**(4)** Check the box if qualifies for (see instructions): Child tax credit	Credit for other dependents
			☐	☐
			☐	☐
			☐	☐
			☐	☐

Income

Attach Form(s) W-2 here. Also attach Forms W-2G and 1099-R if tax was withheld.

If you did not get a Form W-2, see instructions.

Attach Sch. B if required.

Standard Deduction for—
- Single or Married filing separately, $12,950
- Married filing jointly or Qualifying surviving spouse, $25,900
- Head of household, $19,400
- If you checked any box under *Standard Deduction*, see instructions.

1a	Total amount from Form(s) W-2, box 1 (see instructions)				1a
b	Household employee wages not reported on Form(s) W-2				1b
c	Tip income not reported on line 1a (see instructions)				1c
d	Medicaid waiver payments not reported on Form(s) W-2 (see instructions)				1d
e	Taxable dependent care benefits from Form 2441, line 26				1e
f	Employer-provided adoption benefits from Form 8839, line 29				1f
g	Wages from Form 8919, line 6				1g
h	Other earned income (see instructions)				1h
i	Nontaxable combat pay election (see instructions)	1i			
z	Add lines 1a through 1h				1z
2a	Tax-exempt interest	2a		b Taxable interest	2b
3a	Qualified dividends	3a		b Ordinary dividends	3b
4a	IRA distributions	4a		b Taxable amount	4b
5a	Pensions and annuities	5a		b Taxable amount	5b
6a	Social security benefits	6a		b Taxable amount	6b
c	If you elect to use the lump-sum election method, check here (see instructions) ☐				
7	Capital gain or (loss). Attach Schedule D if required. If not required, check here ☐				7
8	Other income from Schedule 1, line 10				8
9	Add lines 1z, 2b, 3b, 4b, 5b, 6b, 7, and 8. This is your **total income**				9
10	Adjustments to income from Schedule 1, line 26				10
11	Subtract line 10 from line 9. This is your **adjusted gross income**				11
12	**Standard deduction or itemized deductions** (from Schedule A)				12
13	Qualified business income deduction from Form 8995 or Form 8995-A				13
14	Add lines 12 and 13				14
15	Subtract line 14 from line 11. If zero or less, enter -0-. This is your **taxable income**				15

Tax and Credits

16	**Tax** (see instructions). Check if any from Form(s): **1** ☐ 8814 **2** ☐ 4972 **3** ☐		16
17	Amount from Schedule 2, line 3		17
18	Add lines 16 and 17		18
19	Child tax credit or credit for other dependents from Schedule 8812		19
20	Amount from Schedule 3, line 8		20
21	Add lines 19 and 20		21
22	Subtract line 21 from line 18. If zero or less, enter -0-		22
23	Other taxes, including self-employment tax, from Schedule 2, line 21		23
24	Add lines 22 and 23. This is your **total tax**		24

Payments

25	Federal income tax withheld from:		
a	Form(s) W-2	25a	
b	Form(s) 1099	25b	
c	Other forms (see instructions)	25c	
d	Add lines 25a through 25c		25d
26	2022 estimated tax payments and amount applied from 2021 return		26
27	Earned income credit (EIC)	27	
28	Additional child tax credit from Schedule 8812	28	
29	American opportunity credit from Form 8863, line 8	29	
30	Reserved for future use	30	
31	Amount from Schedule 3, line 15	31	
32	Add lines 27, 28, 29, and 31. These are your **total other payments and refundable credits**		32
33	Add lines 25d, 26, and 32. These are your **total payments**		33

If you have a qualifying child, attach Sch. EIC.

Refund

34	If line 33 is more than line 24, subtract line 24 from line 33. This is the amount you **overpaid**		34
35a	Amount of line 34 you want **refunded to you**. If Form 8888 is attached, check here ☐		35a
b	Routing number	**c** Type: ☐ Checking ☐ Savings	
d	Account number		
36	Amount of line 34 you want **applied to your 2023 estimated tax**	36	

Direct deposit? See instructions.

Amount You Owe

37	Subtract line 33 from line 24. This is the **amount you owe**. For details on how to pay, go to *www.irs.gov/Payments* or see instructions		37
38	Estimated tax penalty (see instructions)	38	

Third Party Designee

Do you want to allow another person to discuss this return with the IRS? See instructions ☐ **Yes.** Complete below. ☐ **No**

Designee's name | Phone no. | Personal identification number (PIN)

Sign Here

Under penalties of perjury, I declare that I have examined this return and accompanying schedules and statements, and to the best of my knowledge and belief, they are true, correct, and complete. Declaration of preparer (other than taxpayer) is based on all information of which preparer has any knowledge.

Your signature	Date	Your occupation	If the IRS sent you an Identity Protection PIN, enter it here (see inst.)
Spouse's signature. If a joint return, **both** must sign.	Date	Spouse's occupation	If the IRS sent your spouse an Identity Protection PIN, enter it here (see inst.)
Phone no.	Email address		

Joint return? See instructions. Keep a copy for your records.

Paid Preparer Use Only

Preparer's name	Preparer's signature	Date	PTIN	Check if: ☐ Self-employed
Firm's name				Phone no.
Firm's address				Firm's EIN

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Get Ready now to file your 2022 federal income tax return

IR-2022-203, Nov. 22, 2022

WASHINGTON — The Internal Revenue Service today encouraged taxpayers to take simple steps before the end of the year to make filing their 2022 federal tax return easier. With a little advance preparation, a preview of tax changes and convenient online tools, taxpayers can approach the upcoming tax season with confidence.

Filers can visit the Get Ready webpage at IRS.gov/getready to find guidance on what's new and what to consider when filing a 2022 tax return. They can also find helpful information on organizing tax records and a list of online tools and resources.

Get Ready by gathering tax records

When filers have all their tax documentation gathered and organized, they're in the best position to file an accurate return and avoid processing or refund delays or receiving IRS letters. Now's a good time for taxpayers to consider financial transactions that occurred in 2022, if they're taxable and how they should be reported.

The IRS encourages taxpayers to develop an electronic or paper recordkeeping system to store tax-related information in one place for easy access. Taxpayers should keep copies of filed tax returns and their supporting documents for at least three years.

Before January, taxpayers should confirm that their employer, bank and other payers have their current mailing address and email address to ensure they receive their year-end financial statements. Typically, year-end forms start arriving by mail or are available online in mid-to-late January. Taxpayers should carefully review each income statement for accuracy and contact the issuer to correct information that needs to be updated.

Get Ready for what's new for Tax Year 2022

With the end of the year approaching, time is running out to take advantage of the Tax Withholding Estimator on IRS.gov. This online tool is designed to help taxpayers determine the right amount of tax to have withheld from their paycheck. Some people may have life changes like getting married or divorced, welcoming a child or taking on a second job. Other taxpayers may need to consider estimated tax payments due to non-wage income from unemployment, self-employment, annuity income or even digital assets. The last quarterly payment for 2022 is due on Jan. 17, 2023. The Tax Withholding Estimator on IRS.gov can help wage earners determine if there is a need to adjust their withholding, consider additional tax payments, or submit a new W-4 form to their employer to avoid an unexpected tax bill when they file.

As taxpayers gather tax records, they should remember that most income is taxable. This includes unemployment income, refund interest and income from the gig economy and digital assets.

Taxpayers should report the income they earned, including from part-time work, side jobs or the sale of goods. The American Rescue Plan Act of 2021 lowered the reporting threshold for third-party networks that process payments for those doing business. Prior to 2022, Form 1099-K was issued for third-party payment network transactions only if the total number of transactions exceeded 200 for the year and the aggregate amount of these transactions exceeded $20,000. Now a single transaction exceeding $600 can trigger a 1099-K. The lower information reporting threshold and the summary of income on Form 1099-K enables taxpayers to more easily track the amounts received. Remember, money received through third-party payment applications from friends and relatives as personal gifts or reimbursements for personal expenses is not taxable. Those who receive a 1099-K reflecting income they didn't earn should call the issuer. The IRS cannot correct it.

Credit amounts also change each year like the Child Tax Credit (CTC), Earned Income Tax Credit (EITC) and Dependent Care Credit. Taxpayers can use the Interactive Tax Assistant on IRS.gov to determine their eligibility for tax credits. Some taxpayers may qualify this year for the expanded eligibility for the Premium Tax Credit, while others may qualify for a Clean Vehicle Credit through the Inflation Reduction Act of 2022.

Refunds may be smaller in 2023. Taxpayers will not receive an additional stimulus payment with a 2023 tax refund because there were no Economic Impact Payments for 2022. In addition, taxpayers who don't itemize and take the standard deduction, won't be able to deduct their charitable contributions.

The IRS cautions taxpayers not to rely on receiving a 2022 federal tax refund by a certain date, especially when making major purchases or paying bills. Some returns may require additional review and may take longer. For example, the IRS and its partners in the tax industry, continue to strengthen security reviews to protect against identity theft. Additionally, refunds for people claiming the Earned Income Tax Credit (EITC) or the Additional Child Tax Credit (ACTC) can't be issued before mid-February. The law requires the IRS to hold the entire refund – not just the portion associated with EITC or ACTC. This law helps ensure taxpayers receive the refund they're due by giving the IRS time to detect and prevent fraud.

For taxpayers who are still waiting for confirmation that last year's tax return processed, or for a tax year 2021 refund or stimulus payment to process, their patience is appreciated. As of Nov. 11, 2022, the IRS had 3.7 million unprocessed individual returns received this year. These include tax year 2021 returns and late filed prior year returns. Of these, 1.7 million returns require error correction or other special handling, and 2 million are paper returns waiting to be reviewed and processed. They also had 900,000 unprocessed Forms 1040-X for amended tax returns. The IRS is processing these amended returns in the order received and the current timeframe can be more than 20 weeks. Taxpayers should continue to check Where's My Amended Return? for the most up-to-date processing status available.

Renew expiring tax ID numbers

Taxpayers should ensure their Individual Tax Identification Number (ITIN) hasn't expired before filing a 2022 tax return. Those who need to file a tax return, should submit a Form W-7, Application for IRS Individual Taxpayer Identification Number now, to renew their ITIN. Taxpayers who fail to renew an ITIN before filing a tax return next year could face a delayed refund and may be ineligible for certain tax credits. Applying now will help avoid the rush as well as refund and processing delays in 2023.

Bookmark the following tools on IRS.gov

Online tools are easy to use and available to taxpayers 24 hours a day. They provide key information about tax accounts and a convenient way to pay taxes. IRS.gov provides information in many languages and enhanced services for people with disabilities, including the Accessibility Helpline. Taxpayers who need accessibility assistance may call 833-690-0598. Taxpayers should use IRS.gov as their first and primary resource for accurate tax information.

- **Let Us Help You page**. The Let Us Help You page on IRS.gov has links to information and resources on a wide range of topics.
- **Online Account**. An IRS online account lets taxpayers securely access their personal tax information, including tax return transcripts, payment history, certain notices, prior year adjusted gross income and power of attorney information. Filers can log in to verify if their name and address is correct. They should notify IRS if their address has changed. They must notify the Social Security Administration of a legal name change to avoid a delay in processing their tax return.
- **IRS Free File**. Almost everyone can file electronically for free on IRS.gov/freefile or with the IRS2Go app. The IRS Free File program, available only through IRS.gov, offers brand-name tax preparation software packages at no cost. The software does all the work of finding deductions, credits and exemptions for filers. It's free for those who qualify. Some Free File packages offer

free state tax return preparation. Those who are comfortable preparing their own taxes can use Free File Fillable Forms, regardless of their income, to file their tax return either online or by mail.

- **Find a tax professional**. The Choosing a Tax Professional page on IRS.gov has a wealth of information to help filers choose a tax professional. In addition, the Directory of Federal Tax Return Preparers with Credentials and Select Qualifications can help taxpayers find preparers in their area who hold professional credentials recognized by the IRS, or who hold an Annual Filing Season Program Record of Completion.
- **Interactive Tax Assistant.** The Interactive Tax Assistant is a tool that provides answers to many tax questions. It can determine if a type of income is taxable and eligibility to claim certain credits or deductions. It also provides answers for general questions, such as determining filing requirement, filing status or eligibility to claim a dependent.
- **Where's My Refund?** Taxpayers can use the Where's My Refund? tool to check the status of their refund. Current year refund information is typically available online within 24 hours after the IRS receives an e-filed tax return. A paper return status can take up to four weeks to appear after it is mailed. The *Where's My Refund?* tool updates once every 24 hours, usually overnight, so filers only need to check once a day.
- **Volunteer Income Tax Assistance**. The Volunteer Income Tax Assistance (VITA) and Tax Counseling for the Elderly (TCE) programs offer free basic tax return preparation to qualified individuals.

Get refunds fast with Direct Deposit

Taxpayers should prepare to file electronically and choose Direct Deposit for their tax refund – it's the fastest and safest way to file and get a refund. Even when filing a paper return, choosing a direct deposit refund can save time. For those who do not have a bank account, the FDIC website offers information to help people open an account online.

Taxpayers can download Publication 5349, Tax Preparation is for Everyone, for more information to help them get ready to file.

— 30 —

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Reminder to IRA owners age 70½ or over: Qualified charitable distributions are great options for making tax-free gifts to charity

IR-2022-201, Nov. 17, 2022

WASHINGTON —The Internal Revenue Service today reminded IRA owners age 70½ or over of their option to transfer up to $100,000 to charity tax-free each year.

These transfers, known as qualified charitable distributions or QCDs, offer eligible older Americans a great way to easily give to charity before the end of the year. Moreover, for those who are at least 72, QCDs count toward the IRA owner's required minimum distribution (RMD) for the year.

How to set up a QCD

Any IRA owner who wishes to make a QCD for 2022 should contact their IRA trustee soon so the trustee will have time to complete the transaction before the end of the year.

Normally, distributions from a traditional individual retirement arrangement (IRA) are taxable when received. With a QCD, however, these distributions become tax-free as long as they're paid directly from the IRA to an eligible charitable organization.

QCDs can be made electronically, directly to the charity, or by check payable to the charity.

An IRA distribution, such as an electronic payment made directly to the IRA owner, does not count as a QCD. Likewise, a check made payable to the IRA owner is not a QCD.

Each year, an IRA owner **age 70½ or over** can exclude from gross income up to $100,000 of these QCDs. For a married couple, if both spouses are **age 70½ or over and both have IRAs,** each spouse can exclude up to $100,000 for a total of up to $200,000 per year.

The QCD option is available regardless of whether an eligible IRA owner itemizes deductions on Schedule A. Transferred amounts are not taxable, and no deduction is available for the transfer.

Report correctly

A 2022 QCD must be reported on the 2022 federal income tax return, normally filed during the 2023 tax filing season.

In early 2023, the IRA owner will receive Form 1099-R from their IRA trustee that shows any IRA distributions made during calendar year 2022, including both regular distributions and QCDs. The total distribution is in Box 1 on that form. There is no special code for a QCD.

Like other IRA distributions, QCDs are shown on Line 4 of Form 1040 or Form 1040-SR. If part or all of an IRA distribution is a QCD, enter the total amount of the IRA distribution on Line 4a. This is the amount shown in Box 1 on Form 1099-R.

Then, if the full amount of the distribution is a QCD, enter 0 on Line 4b. If only part of it is a QCD, the remaining taxable portion is normally entered on Line 4b.

Either way, be sure to enter "QCD" next to Line 4b. Further details will be in the final instructions to the 2022 Form 1040.

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Get a receipt

QCDs are not deductible as charitable contributions on Schedule A. But, as with deductible contributions, the donor must get a written acknowledgement of their contribution from the charitable organization, before filing their return.

In general, the acknowledgement must state the date and amount of the contribution and indicate whether the donor received anything of value in return. For details, see the Acknowledgement section in Publication 526, available on IRS.gov.

For more information about IRA distributions and QCDs, see Publication 590-B, also available on IRS.gov.

-30-

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

IRS increases mileage rate for remainder of 2022

IR-2022-124, June 9, 2022

WASHINGTON — The Internal Revenue Service today announced an increase in the optional standard mileage rate for the final 6 months of 2022. Taxpayers may use the optional standard mileage rates to calculate the deductible costs of operating an automobile for business and certain other purposes.

For the final 6 months of 2022, the standard mileage rate for business travel will be 62.5 cents per mile, up 4 cents from the rate effective at the start of the year. The new rate for deductible medical or moving expenses (available for active-duty members of the military) will be 22 cents for the remainder of 2022, up 4 cents from the rate effective at the start of 2022. These new rates become effective July 1, 2022. The IRS provided legal guidance on the new rates in Announcement 2022-13, issued today.

In recognition of recent gasoline price increases, the IRS made this special adjustment for the final months of 2022. The IRS normally updates the mileage rates once a year in the fall for the next calendar year. For travel from Jan. 1 through June 30, 2022, taxpayers should use the rates set forth in Notice 2022-03.

"The IRS is adjusting the standard mileage rates to better reflect the recent increase in fuel prices," said IRS Commissioner Chuck Rettig. "We are aware a number of unusual factors have come into play involving fuel costs, and we are taking this special step to help taxpayers, businesses and others who use this rate."

While fuel costs are a significant factor in the mileage figure, other items enter into the calculation of mileage rates, such as depreciation and insurance and other fixed and variable costs.

The optional business standard mileage rate is used to compute the deductible costs of operating an automobile for business use in lieu of tracking actual costs. This rate is also used as a benchmark by the federal government and many businesses to reimburse their employees for mileage.

Taxpayers always have the option of calculating the actual costs of using their vehicle rather than using the standard mileage rates.

The 14 cents per mile rate for charitable organizations remains unchanged as it is set by statute.

Midyear increases in the optional mileage rates are rare, the last time the IRS made such an increase was in 2011.

Mileage Rate Changes

Purpose	Rates 1/1 through 6/30/22	Rates 7/1 through 12/31/22
Business	58.5	62.5
Medical/Moving	18	22
Charitable	14	14

-30-

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

401(k) limit increases to $22,500 for 2023, IRA limit rises to $6,500

IR-2022-188, Oct. 21, 2022

WASHINGTON — The Internal Revenue Service announced today that the amount individuals can contribute to their 401(k) plans in 2023 has increased to $22,500, up from $20,500 for 2022. The IRS today also issued technical guidance regarding all of the cost-of-living adjustments affecting dollar limitations for pension plans and other retirement-related items for tax year 2023 in Notice 2022-55, posted today on IRS.gov.

Highlights of changes for 2023

The contribution limit for employees who participate in 401(k), 403(b), most 457 plans, and the federal government's Thrift Savings Plan is increased to $22,500, up from $20,500.

The limit on annual contributions to an IRA increased to $6,500, up from $6,000. The IRA catch-up contribution limit for individuals aged 50 and over is not subject to an annual cost-of-living adjustment and remains $1,000.

The catch-up contribution limit for employees aged 50 and over who participate in 401(k), 403(b), most 457 plans, and the federal government's Thrift Savings Plan is increased to $7,500, up from $6,500. Therefore, participants in 401(k), 403(b), most 457 plans, and the federal government's Thrift Savings Plan who are 50 and older can contribute up to $30,000, starting in 2023. The catch-up contribution limit for employees aged 50 and over who participate in SIMPLE plans is increased to $3,500, up from $3,000.

The income ranges for determining eligibility to make deductible contributions to traditional Individual Retirement Arrangements (IRAs), to contribute to Roth IRAs, and to claim the Saver's Credit all increased for 2023.

Taxpayers can deduct contributions to a traditional IRA if they meet certain conditions. If during the year either the taxpayer or the taxpayer's spouse was covered by a retirement plan at work, the deduction may be reduced, or phased out, until it is eliminated, depending on filing status and income. (If neither the taxpayer nor the spouse is covered by a retirement plan at work, the phase-outs of the deduction do not apply.) Here are the phase-out ranges for 2023:

- For single taxpayers covered by a workplace retirement plan, the phase-out range is increased to between $73,000 and $83,000, up from between $68,000 and $78,000.
- For married couples filing jointly, if the spouse making the IRA contribution is covered by a workplace retirement plan, the phase-out range is increased to between $116,000 and $136,000, up from between $109,000 and $129,000.
- For an IRA contributor who is not covered by a workplace retirement plan and is married to someone who is covered, the phase-out range is increased to between $218,000 and $228,000, up from between $204,000 and $214,000.

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

- For a married individual filing a separate return who is covered by a workplace retirement plan, the phase-out range is not subject to an annual cost-of-living adjustment and remains between $0 and $10,000.

The income phase-out range for taxpayers making contributions to a Roth IRA is increased to between $138,000 and $153,000 for singles and heads of household, up from between $129,000 and $144,000. For married couples filing jointly, the income phase-out range is increased to between $218,000 and $228,000, up from between $204,000 and $214,000. The phase-out range for a married individual filing a separate return who makes contributions to a Roth IRA is not subject to an annual cost-of-living adjustment and remains between $0 and $10,000.

The income limit for the Saver's Credit (also known as the Retirement Savings Contributions Credit) for low- and moderate-income workers is $73,000 for married couples filing jointly, up from $68,000; $54,750 for heads of household, up from $51,000; and $36,500 for singles and married individuals filing separately, up from $34,000.

The amount individuals can contribute to their SIMPLE retirement accounts is increased to $15,500, up from $14,000.

Details on these and other retirement-related cost-of-living adjustments for 2023 are in Notice 2022-55, available on IRS.gov.

-30-

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Reminder: Service providers, others may receive 1099-Ks for sales over $600 in early 2023

IR-2022-189, Oct. 24, 2022

WASHINGTON — The Internal Revenue Service reminds taxpayers earning income from selling goods and/or providing services that they may receive Form 1099-K, Payment Card and Third-Party Network Transactions, for payment card transactions and third-party payment network transactions of more than $600 for the year.

There is no change to the taxability of income; the only change is to the reporting rules for Form 1099-K. As before, income, including from part-time work, side jobs or the sale of goods, is still taxable. Taxpayers must report all income on their tax return unless it is excluded by law, whether they receive a Form 1099-NEC, Nonemployee Compensation; Form 1099-K; or any other information return.

The IRS emphasizes that money received through third-party payment applications from friends and relatives as personal gifts or reimbursements for personal expenses is not taxable.

The American Rescue Plan Act of 2021 (ARPA) lowered the reporting threshold for third-party networks that process payments for those doing business. Prior to 2022, Form 1099-K was issued for third party payment network transactions only if the total number of transactions exceeded 200 for the year and the aggregate amount of these transactions exceeded $20,000. Now a single transaction exceeding $600 can trigger a 1099-K.

The lower information reporting threshold and the summary of income on Form 1099-K enables taxpayers to more easily track the amounts received.

Generally, greater income reporting accuracy by taxpayers also lowers the need and likelihood of later examination.

Consider making estimated tax payment

Income taxes must generally be paid as taxpayers earn or receive income throughout the year, either through withholding or estimated tax payments.

If the amount of income tax withheld from one's salary or pension is not enough, or if they receive other types of income, such as interest, dividends, alimony, self-employment income, capital gains, prizes and awards, they may have to make estimated tax payments.

If they are in business for themselves, individuals generally need to make estimated tax payments. Estimated tax payments are used to pay not only income tax, but other taxes as well, such as self-employment tax and alternative minimum tax.

Publication 17, Your Federal Income Tax (for Individuals), provides general rules to help taxpayers pay the income taxes they owe.

Additional helpful information is available in Chapter 5, Business Income, of Publication 334, Tax Guide for Small Business; Publication 525, Taxable and Nontaxable Income and on IRS.gov at Understanding Your Form 1099-K.

Form 1099-K, its instructions and a set of answers to frequently asked questions are available on IRS.gov.

-30-

IRS Fact Sheet
Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Money received through 'crowdfunding' may be taxable; taxpayers should understand their obligations and the benefits of good recordkeeping

FS-2022-20, March 2022

Understanding Crowdfunding
Crowdfunding is a method of raising money through websites by soliciting contributions from a large number of people. The contributions may be solicited to fund businesses, for charitable donations, or for gifts. In some cases, the money raised through crowdfunding is solicited by crowdfunding organizers on behalf of other people or businesses. In other cases, people establish crowdfunding campaigns to raise money for themselves or their businesses.

Receipt of a Form 1099-K for Distributions of Money Raised Through Crowdfunding
The crowdfunding website or its payment processor may be required to report distributions of money raised if the amount distributed meets certain reporting thresholds by filing Form 1099-K, *Payment Card and Third Party Network Transactions*, with the IRS. If Form 1099-K is required to be filed with the IRS, the crowdfunding website or its payment processor must also furnish a copy of that form to the person to whom the distributions are made. The American Rescue Plan Act clarifies that the crowdfunding website or its payment processor is not required to file Form 1099-K with the IRS or furnish it to the person to whom the distributions are made if the contributors to the crowdfunding campaign do not receive goods or services for their contributions.

Prior to 2022, the threshold for a crowdfunding website or payment processor to file and furnish a Form 1099-K was met if, during a calendar year, the total of all payments distributed to a person exceeded $20,000 in gross payments resulting from more than 200 transactions or donations.

For calendar years beginning after December 31, 2021, the threshold is lowered and is met if, during a calendar year, the total of all payments distributed to a person exceeds $600 in gross payments, regardless of the number of transactions or donations.

Accordingly, if a crowdfunding website or its payment processor makes distributions of money raised that meet the reporting threshold, and the contributors to the crowdfunding campaign received goods or services for their contributions, then a Form 1099-K is required to be filed with the IRS. Additionally, if the distributions of the money raised are made to the crowdfunding organizer, a copy of the Form 1099-K must be furnished to the organizer; alternatively, if the distributions of the money raised are made directly to individuals or businesses for whom the organizer solicited funds, the Form 1099-K must be furnished to those individuals or businesses that receive amounts that meet the reporting threshold.

A person receiving a Form 1099-K for distributions of money raised through crowdfunding may not recognize the filer's name on the form. Sometimes the payment processor used by the crowdfunding website, rather than the crowdfunding website itself, will issue the Form 1099-K and be included as the filer on the form. If the recipient of a Form 1099-K does not recognize the filer's name or the amounts included on the Form 1099-K, the recipient can use the filer's telephone number listed on the form to contact a person knowledgeable about the payments reported.

Box 1 on the Form 1099-K will show the gross amount of the distributions made to a person during the calendar year, but issuance of a Form 1099-K doesn't automatically mean the amount reported on the form is taxable to the person receiving the form. As discussed below, the income tax consequences depend on all the facts and circumstances. If the distributions reported on a Form 1099-K are not reported on the tax return of

the recipient of the form, the IRS may contact the recipient for more information. The recipient will have the opportunity to explain why the crowdfunding distributions were not reported on the recipient's tax return.

Tax Treatment of Money Raised Through Crowdfunding
Under federal tax law, gross income includes all income from whatever source derived unless it is specifically excluded from gross income by law. In most cases, property received as a gift is not includible in the gross income of the person receiving the gift.

If a crowdfunding organizer solicits contributions on behalf of others, distributions of the money raised to the organizer may not be includible in the organizer's gross income if the organizer further distributes the money raised to those for whom the crowdfunding campaign was organized.

If crowdfunding contributions are made as a result of the contributors' detached and disinterested generosity, and without the contributors receiving or expecting to receive anything in return, the amounts may be gifts and therefore may not be includible in the gross income of those for whom the campaign was organized. Contributions to crowdfunding campaigns are not necessarily a result of detached and disinterested generosity, and therefore may not be gifts. Additionally, contributions to crowdfunding campaigns by an employer to, or for the benefit of, an employee are generally includible in the employee's gross income.

Taxpayers may want to consult a trusted tax professional for information and advice regarding how to treat amounts received from crowdfunding campaigns.

Recordkeeping for Money Raised Through Crowdfunding
Crowdfunding organizers and any person receiving amounts from crowdfunding should keep complete and accurate records of all facts and circumstances surrounding the fundraising and disposition of funds for at least three years.

Links
About Form 1099-K, Payment Card and Third Party Network Transactions
Understanding Your Form 1099-K
General FAQs on Payment Card and Third Party Network Transactions
Gig Economy Tax Center

–30–

IRS Fact Sheet

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Know the difference between a hobby and a business

FS-2022-38, October 2022

Most people take up hobbies for personal enjoyment, not to make a profit. Sometimes, however, the line between hobbies and businesses isn't clear cut. There are several different factors people should consider when making the determination and the IRS provides resources to help.

The following information is available on IRS.gov to help a taxpayer determine if their hobby qualifies as a business:

- Business Activities
- Five Things to Remember about Hobby Income
- Earning side income: is it a hobby or a business?

Key questions to consider

Is the activity conducted like a business?

- Does the taxpayer maintain complete and accurate books and records?
- Does the taxpayer do the activity in the same way as similar profitable activities?

Does the taxpayer change their methods of operation to improve profitability?

- Does the taxpayer advertise or promote the activity?
- Does the taxpayer work to secure suppliers or products necessary for the activity?

What is the taxpayer or their advisors' expertise in the activity?

- Has the taxpayer, or their advisors, prepared for the activity by extensive study of its accepted business, economic, and scientific practices?
- Does the taxpayer follow the accepted business practices or advice of experts when they pursue the activity?

Is the activity a main source of income for the taxpayer?

- Does the taxpayer spend much of their personal time and effort on the activity, particularly if the activity does not have personal or recreational aspects?
- Has the taxpayer pursued the activity full-time or part-time?
- Does the taxpayer employ competent and qualified persons to perform the activity?

Has the taxpayer made or expect to make a profit?

- Has the taxpayer engaged in similar activities in the past and converted them from unprofitable to profitable enterprises?
- Does the taxpayer intend to profit from appreciation in the value of assets, such as land, used in the activity?

Is the activity profitable in some years?

- Does the taxpayer occasionally have a small profit from the activities that is offset by large investments they have made or suffering large losses?
- Has the taxpayer made substantial profit from the activity?
- Could the activity earn a substantial ultimate profit in a highly speculative venture?

Do any losses from the activity fall beyond the taxpayer's control or are they normal in the startup phase of their type of business?

- Do the taxpayer's losses continue beyond the period which would be necessary to bring their activity into profitable status?
- Are the taxpayer's losses because of things beyond their control, like drought, disease, fire, theft, weather damages or depressed market conditions?
- Has the taxpayer had a series of years in which they made a profit?

Does the activity have elements of personal pleasure or recreation?

- Does the taxpayer have personal motives for doing an activity, especially where there are recreational or personal elements involved?
- Does the activity lack appeal other than profit?

Claiming profits and losses

If taxpayers aren't trying to make a profit with their hobby, business or investment activity, they can't use a loss from the activity to offset other income. The limit on not-for-profit losses applies to individuals, partnerships, estates, trusts and S corporations. It doesn't apply to corporations other than S corporations.

If a taxpayer receives income from an activity that is carried on with no intention of making a profit, they must report the income they receive on Schedule 1, Form 1040, line 8.

More information:

- IRS Small Business Self-Employed Tax Center YouTube Video
- Income & Expenses | Internal Revenue Service (irs.gov)
- Gig Economy Tax Center
- IRS Video Portal
- Publication 17, Your Federal Income Tax
- Publication 525, Taxable and Nontaxable Income
- Publication 535, Business Expenses
- Publication 334, Tax Guide for Small Business (For Individuals Who Use Schedule C)

Virtual Currency

Have questions about virtual currency? Check out IRS.gov

The IRS uses the term “virtual currency” to describe the various types of virtual currency that are used as a medium of exchange, such as digital currency and cryptocurrency. Regardless of the label applied, if a particular asset has the characteristics of virtual currency, it will be treated as virtual currency for federal income tax purposes.

Virtual currency transaction reporting

When you sell, exchange, or use virtual currency, to pay for goods or services, or otherwise dispose of virtual currency, you must report this to the IRS. For more information on capital assets, capital gains, and capital losses, see **Publication 544, Sales and Other Dispositions of Assets**.

Record keeping

You must maintain records documenting receipts, sales, exchanges or other dispositions of virtual currency and the fair market value of the virtual currency.

Visit the virtual currencies page on IRS.gov for more information.

How to Submit Authorizations Using Tax Pro Account and Online Account

1. Steps for the Tax Professional

- Log in to Tax Pro Account at **www.irs.gov/taxproaccount** after validating identity.
- Initiate request for either a power of attorney (POA) or tax information authorization (TIA).
- Enter tax professional's information – name, address, and Centralized Authorization File (CAF) number.
- Enter taxpayer's information – name, address, and tax identification number (TIN).
- Select tax matter(s) and tax period(s).
- Check box as electronic signature (for POA only) and submit authorization for IRS validation and routing to taxpayer's Online Account.
- Inform taxpayer that an authorization request should be pending in their Online Account for their review and approval.

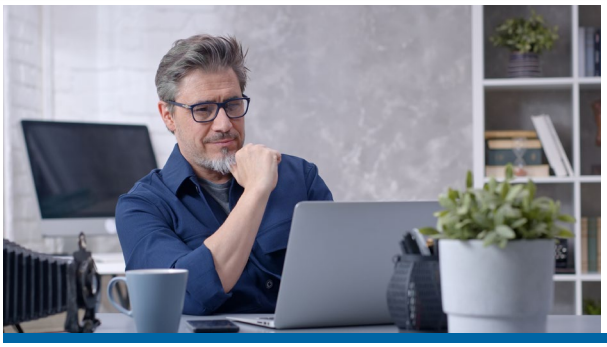
2. Steps for the Taxpayer

- Log in to Online Account at **www.irs.gov/account** after validating identity.
- Select the "Authorizations" tab.
- Review request from tax professional for accuracy.
- Check box as digital signature and approve the request; taxpayer also has the option to reject the request.

3. Most requests record immediately to the CAF database; will show as approved in Online Account and Tax Pro Account.

Tips

- Tax professional and taxpayer names and addresses must match IRS records exactly.
- Tax professional must already have a CAF number and be in good standing with the IRS.
- Tax Pro Account is available to tax professionals and taxpayers with addresses in the United States.
- Prior authorization revoked when new request is recorded for same request type, tax matter and period.
- Taxpayers maintain control over who can represent them before IRS or see their IRS tax records.



Benefits of Tax Pro Account and Digital Authorizations

All-digital authorization process improves service to taxpayers by offering real-time posting to the Centralized Authorization File (CAF). Tax Professionals: Make Tax Pro Account your primary tool for CAF.

Tax Pro Account Benefits:

- Provides all-digital process to initiate and sign authorization requests
- Records most authorizations immediately to CAF; some may take 48 hours
- Eliminates manual reviews, allowing faster service for taxpayers
- Allows for electronic signatures; taxpayers simply check a box and submit to CAF
- Revokes prior authorizations for same request type, tax matter and period
- Enhances identity protection by requiring IRS e-authentication for both parties

How Tax Pro Account Works:

- Tax professional accesses Tax Pro Account with IRS username and password
  - Initiates Power of Attorney (POA) or Tax Information Authorization (TIA)
  - Enters personal information exactly as entered on most recent tax return
  - Checks box for digital signatures on a POA
  - Submits to electronically transfer request to taxpayer's Online Account
- Taxpayer accesses Online Account with IRS username and password
  - Selects "Authorization" tab, reviews request
  - Checks box for approval or may also reject
  - Submits approved request directly to CAF
- Recorded authorizations display in both Tax Pro Account and Online Account
- Tax professional accesses e-Services' Transcript Delivery System as needed

What Tax Professionals Need to Know:

- Taxpayers must register for Online Account
- Tax professionals must already have a CAF number and be in good standing with the IRS.
- Limited to individual clients only; entities must use fax, mail or the online submission
- Authorizations can have multiple representatives/designees; follow correct process
- Available only to tax professionals and taxpayers with addresses in the United States
- New features will be added to Tax Pro Account, enhancing online connections to clients

Resources to share with clients:

Publication 5533, Why You Should Create an IRS Online Account
Publication 5533-A, How to Submit Authorizations Using Tax Pro Account and Online Account

For more information, visit www.irs.gov/taxproaccount and www.irs.gov/account.

Online Account
www.irs.gov/account

Why You Should Create an IRS Online Account

New Feature
- Use the "authorization" option in Online Account to control who can represent you before the IRS or view your tax records.
- Approve and electronically sign Power of Attorney and Tax Information Authorization requests made by your tax professional.

Access Tax Records
- View key data from your most recent tax return.
- Access additional records via Get Transcript.
- View your Economic Impact Payment amounts.

View Balance and Notices
- View amount owed.
- Access digital versions of select correspondence from the IRS.

Payment Plans
- Learn about payment plan options.
- View payment plan details.

Make and View Payments
- Make a payment from your bank account or by debit/credit card.
- View five years of payment history and any pending or scheduled payments.

Upcoming Feature

Update Profile
- View and update address on file.
- Manage preferences such as email notifications.

Upcoming Feature

Opt-Out of Paper Notices
- Go paperless for certain correspondence from the IRS.

Create or access your account at www.irs.gov/account.

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

IRS unveils new online identity verification process for accessing self-help tools

IR-2021-228, Nov. 17, 2021

WASHINGTON – The Internal Revenue Service today announced the launch of an improved identity verification and sign-in process that enables more people to securely access and use IRS online tools and applications.

Taxpayers using the new mobile-friendly verification procedure can gain entry to existing IRS online services such as the Child Tax Credit Update Portal, Online Account, Get Transcript Online, Get an Identity Protection PIN (IP PIN) and Online Payment Agreement. Additional IRS applications will transition to the new method over the next year.

“Identity verification is critical to protect taxpayers and their information. The IRS has been working hard to make improvements in this area, and this new verification process is designed to make IRS online applications as secure as possible for people,” said IRS Commissioner Chuck Rettig. “To help taxpayers and the tax community, we are improving the accessibility of online tools that help families manage their Child Tax Credit, check on their IRS accounts and securely perform other routine tasks online.”

The new process can reach more people through the expanded use of identity documents and increased help desk assistance for taxpayers who encounter a problem when attempting to verify their identity online. Developed under the Secure Access Digital Identity initiative (SADI), the new process complies with a federal mandate.

To provide verification services, the IRS is using ID.me, a trusted technology provider. The new process is one more step the IRS is taking to ensure that taxpayer information is provided only to the person who legally has a right to the data.

The IRS also integrated this new account-creation process into some applications used by tax professionals, including those used to request powers of attorney or tax information authorizations online using Tax Pro Account or to submit Forms 2848 and 8821 online.

Accessing IRS tools

When accessing the tools listed above, taxpayers will be asked to sign in with an ID.me account. People who already have IRS usernames may continue to use their credentials from the old system to sign-in until summer 2022, but are prompted to create an ID.me account as soon as possible. Anyone with an existing ID.me account from the Child Tax Credit Update Portal, or from another government agency, can sign in with their existing credentials.

To verify their identity with ID.me, taxpayers need to provide a photo of an identity document such as a driver’s license, state ID or passport. They’ll also need to take a selfie with a smartphone or a computer with a webcam. Once their identity has been verified, they can securely access IRS online services.

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Taxpayers who need help verifying their identity or submitting a support ticket can visit the ID.me IRS Help Site.

-30-

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Security Summit offers tools, tips to tax pros during National Tax Security Awareness Week; highlights importance of security plans

IR-2022-209, Nov. 30, 2022

WASHINGTON – With tax season quickly approaching, the Internal Revenue Service and the Security Summit partners today urged tax professionals to remain focused on security issues and to review resources available to them, including sample security plans and checklists.

During National Tax Security Awareness Week, now in its seventh year, the Security Summit partnership of the IRS, state tax agencies and the tax software and tax professional communities work to highlight data security and provide scam prevention tips. Part of the Summit's effort continues to be focusing tax professionals, including smaller practices, on ways to protect themselves and safeguard client information. Day three of this special week focuses on several important aspects for the tax community to keep in mind.

"Taxpayer information can be a gold mine for identity thieves. As the Security Summit partners strengthened our internal defenses in recent years, we've seen identity thieves shift their focus onto the tax professional community and their client information," said IRS Acting Commissioner Doug O'Donnell. "Specific taxpayer information can help a scammer prepare a more authentic looking tax return, so tax professionals maintaining strong security is a critical line of defense for themselves, their clients and the nation's tax system."

Written Information Security Plan (WISP)

The IRS and Security Summit partners remind tax professionals that federal law requires them to have a written information security plan. Earlier this year, members of the Summit's tax professional team developed a special document that allows practitioners to quickly develop their own written security plans.

This sample document, a Written Information Security Plan (WISP), can be scaled for a company's size, scope of activities, complexity and customer data sensitivity. There's not a one-size-fits-all WISP. For example, a sole practitioner can use a more abbreviated and simplified plan than a 10-partner accounting firm, which is reflected in the sample WISP from the Security Summit group.

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. But an often overlooked but critical component is creating a WISP.

"There's no way around it for anyone running a tax business. Having a written security plan is a sound business practice – and it's required by law," said Jared Ballew of Drake Software, co-lead for the Summit tax professional team and chair of the Electronic Tax Administration Advisory Committee (ETAAC). "The sample provides a starting point for developing your plan, addresses risk considerations for inclusion in an effective plan and provides a blueprint of applicable actions in the event of a security incident, data losses and theft."

Security issues for a tax professional can be daunting. The Summit team worked to make this document as easy to use as possible, including special sections to help tax professionals get to the information they need.

Here are a few WISP considerations for tax pros:

- Save the WISP in a format others can easily access and read, such as a PDF or Word document.
- Make the WISP available to all employees for training purposes.
- Store a copy offsite or in the cloud in the event of an incident or natural disaster.

Taxes-Security-Together Checklist

Unfortunately, tax practitioners remain high-value targets of cybercriminals seeking to steal sensitive tax information. With this in mind, the Security Summit created the "Taxes-Security-Together" Checklist to help tax professionals identify basic cybersecurity measures to implement.

These six easy steps can make a big difference in protecting information, both for tax pros and taxpayers:

- Use anti-virus software and set it for automatic updates to keep systems secure. This includes all digital products, computers and mobile phones.
- Use firewalls. Firewalls help shield computers from outside attacks but cannot protect systems in cases where users accidentally download malware, for example, from phishing email scams.
- Use multi-factor authentication to protect all online accounts, especially tax products, cloud software providers, email providers and social media.
- Back up sensitive files, especially client data, to secure external sources, such as external hard drive or cloud storage.
- Encrypt data. Tax professionals should consider drive encryption products for full-drive encryption. This will encrypt all data.
- Use a Virtual Private Network (VPN) product. As more practitioners work remotely during the pandemic, a VPN is critical for secure connections.

For more information on how to protect client information, tax professionals should look to Publication 4557, Safeguarding Taxpayer Data.

Phishing scams, malware and ransomware present risks

For both tax professionals and taxpayers, phishing emails generally have an urgent message and try to direct users to an official-looking link or attachment. But the link instead may take users to a fake site made to appear like a trusted source where it requests a username and password. The attachment may also contain malware, which secretly downloads software that tracks keystrokes and allows thieves to eventually steal all the tax professional's passwords.

Some thieves also pose as potential clients and may interact repeatedly with a tax professional and then send an email with an attachment that claims to include their tax information. The attachment may contain malware that allows the thief to track keystrokes and eventually steal all passwords or take over control of the computer systems.

The IRS warns tax pros not to take any of the steps demanded in these types of email, and to delete the email. Recipients of these IRS-related scams can report them to phishing@irs.gov.

Sometimes, phishing scams are ransomware schemes in which the thief gains control of the tax professional's computer systems and holds the data hostage until a ransom is paid. The Federal Bureau of Investigation (FBI) has warned against paying a ransom because thieves often leave the data encrypted.

Security plan requirement and recommended data theft plan

In addition to the required information security plan, tax pros also should consider an emergency response plan should they experience a breach and data theft. This time-saving step should include contact information for the IRS Stakeholder Liaisons, who are the first point of contact for tax professional data theft reporting to the IRS and to the states.

IRS Publication 5293, Data Security Resource Guide for Tax Professionals, provides a compilation of data theft information available on IRS.gov, including the reporting processes.

In addition to reviewing IRS Publication 4557, Safeguarding Taxpayer Data, tax professionals can also get help with security recommendations by reviewing Small Business Information Security: The Fundamentals by the National Institute of Standards and Technology. The IRS Identity Theft Central pages for tax pros, individuals and businesses have important details as well.

Employers can share Publication 4524, Security Awareness for Taxpayers, with their employees and customers and tax professionals can share with clients.

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

For more details on National Tax Security Awareness Week, visit IRS.gov/securitysummit.

-30-

Tax professionals should review their security protocols

As identity thieves continue targeting tax professionals, the IRS and the Summit partners urge practitioners to review the "Taxes-Security-Together" Checklist, including:

- ***Deploy basic security measures.***
- ***Use multi-factor authentication to protect tax software accounts.***
- ***Create a Virtual Private Network if working remotely.***
- ***Create a written data security plan as required by federal law.***
- ***Know about phishing and phone scams.***
- ***Create data security and data theft recovery plans.***

Protect Your Clients; Protect Yourself

Data Security Resource Guide for Tax Professionals

The Data Security Resource Guide for Tax Professionals is intended to provide a basic understanding of minimal steps to protect client data. All tax professionals are encouraged to work with cybersecurity professionals to ensure secure systems. Protecting taxpayer data from theft and disclosure is your responsibility.

Get Started

The Security Summit – the partnership between the Internal Revenue Service, state tax agencies and the tax industry – reminds all tax professionals that everyone has a role in protecting taxpayer data.

The Financial Services Modernization Act of 1999, also known as Gramm-Leach-Bliley Act, requires certain entities – including tax return preparers – to create and maintain a security plan for the protection of client data.

Here are two publications to help you get started:

- **IRS Publication 4557, Safeguarding Taxpayer Data**
  This publication provides an overview of tax professionals' obligations to protect taxpayer information and provides a step-by-step checklist for how to create and maintain a security plan for your digital network and office.
- **NIST's Small Business Information Security – The Fundamentals**
  The National Institute of Standards and Technology (NIST) is a branch of the U.S. Commerce Department. It sets the information security framework for federal agencies. It also produced this document to provide small businesses with an overview of those steps to security data. Its focus is on five principles: identify, protect, detect, respond and recover.

Don't forget **Publication 1345**, Handbook for Authorized IRS e-File Providers, which outlines your responsibility as an Electronic Return Originator, including in the area of e-File security and privacy.

What Can You Do?

- Learn to recognize phishing emails, especially those pretending to be from the IRS, e-Services, a tax software provider or cloud storage provider. Never open a link or any attachment from a suspicious email. Remember: The IRS never initiates initial email contact with tax pros about returns, refunds or requests for sensitive financial or password information.
- Create a data security plan using IRS **Publication 4557**, Safeguarding Taxpayer Data, and **Small Business Information Security – The Fundamentals**, by the National Institute of Standards and Technology.
- Review internal controls:
  - Install anti-malware/anti-virus security software on all devices (laptops, desktops, routers, tablets and phones) and keep software set to automatically update.

- Use strong and unique passwords of 8 or more mixed characters, password protect all wireless devices, use a phrase or words that are easily remembered and change passwords periodically.
- Encrypt all sensitive files/emails and use strong password protections.
- Back up sensitive data to a safe and secure external source not connected fulltime to a network.
- Make a final review of return information – especially direct deposit info - prior to e-filing.
- Wipe clean or destroy old computer hard drives and printers that contain sensitive data.
- Limit access to taxpayer data to individuals who need to know.
- Check IRS e-Services account weekly for number of returns filed with EFIN.

- Report any data thefts or losses to the appropriate IRS Stakeholder Liaison.
- Stay connected to the IRS through subscriptions to e-News for Tax Professionals, QuickAlerts and Social Media.

Learn the Signs of Data Theft

You or your firm may be a victim and not even know it. Here are some common clues to data theft:

- Client e-filed returns begin to reject because returns with their Social Security numbers were already filed;
- 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 account receive an IRS notice that their account was accessed or IRS emails stating their account has been disabled; or, clients receive an IRS notice that an IRS online account was created in their names;
- 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.

Stay Vigilant

Stay ahead of the thieves by taking certain actions daily or weekly to ensure your clients and your business remain safe:

- Track your daily e-File acknowledgements. If there are more acknowledgements than returns you know you filed, dig deeper.

- Track your weekly EFIN usage. The number of returns filed with your Electronic Filing Identification Number (EFIN) is posted weekly. Go to your e-Services account, access your e-file application and check "EFIN Status." If the numbers are off, contact the e-Help desk. Keep your EFIN application up-to-date with all phone, address or personnel changes.
- If you are a 'Circular 230 practitioner' or an 'annual filing season program participant' and you file 50 or more returns a year, you can check your PTIN account for a weekly report of returns filed with your Preparer Tax Identification Number (PTIN.) Access your PTIN account and select "View Returns Filed Per PTIN." File Form 14157, Complaint: Tax Return Preparer, to report excessive using your PTIN or misuse of PTIN.
- If you have a Centralized Authorization File (CAF) Number, make sure you keep your authorizations up to date. Remove authorizations for taxpayers who are no longer your clients. See **Publication 947**, Practice Before the IRS and Power of Attorney.
- Create your IRS online accounts using the two-factor Secure Access authentication, which helps prevent account takeovers. See **IRS.gov/secureaccess** to review necessary steps.

Data Lost or Stolen? Report It Quickly

Contact the IRS and law enforcement:

- **Internal Revenue Service**, report client data theft to your local Stakeholder Liaison.
- **Federal Bureau of Investigation**, your local office (if directed.)
- **Secret Service**, your local office (if directed.)
- Local police – To file a police report on the data breach.

Contact states in which you prepare state returns:

- Email the Federation of Tax Administrators at **StateAlert@taxadmin.org** to get information on how to report victim information to the states.
- **State Attorneys General** for each state in which you prepare returns. Most states require that the attorney general be notified of data breaches.

Contact experts:

- Security expert – to determine the cause and scope of the breach, to stop the breach and to prevent further breaches from occurring.
- Insurance company – to report the breach and to check if your insurance policy covers data breach mitigation expenses.

For a complete checklist, see **Data Theft Information for Tax Professionals**.

Stay Connected

The IRS attempts to alert tax professionals as quickly as possible when it learns of a new scam, which are especially common during the filing season. Sign up so you can stay up to date with the latest alerts and tax administration issues:

- e-News for Tax Professionals – A weekly digest of important tax news geared for tax practitioners
- QuickAlerts – An urgent messaging system regarding e-File for tax professionals who have e-Services accounts.
- IRS social media – The IRS uses several social media outlets to connect with tax pros and with taxpayers. You can follow us at:
  - Twitter.com/IRStaxpros.
  - Twitter.com/IRSnews.
  - Facebook.com/IRStaxpros.

IRS Security Bookmarks:

- Identity Protection: Prevention, Detection and Victim Assistance – Main identity theft page
- Data Theft Information for Tax Professionals – How to report client data loss to the IRS
- Protect Your Clients; Protect Yourself – Awareness campaign and scam alerts for tax pros
- Taxes. Security. Together. – Awareness campaign for taxpayers
- Identity Theft Information for Tax Professionals – An overview
- Report Phishing and Online Scams – How to report IRS-related scams
- How IRS Identity Theft Victim Assistance Works – What clients can expect
- Maintain, Monitor and Protect Your EFIN – Protect your IRS-issued identification numbers
- Secure Access – How to authenticate your identity to access IRS online tools
- Security Summit – Track safeguards enacted by IRS, states and industry
- Newsroom – Stay in the know by subscribing to IRS News Releases
- Stakeholder Liaisons Local Contact – find your local contact to report data losses

How to Create a **Written Information Security Plan** for Data Safety

WISP

With data security incidents continuing, tax professionals must have current written information security plans or WISPs.

Federal law, enforced by the Federal Trade Commission, requires professional tax preparers to create and maintain a written data security plan.

Having a WISP protects businesses and clients while providing a blueprint of action in the event of a security incident. In addition, a WISP can help if other events occur that can seriously disrupt a tax professional's ability to conduct normal business, including fire, flood, tornado, earthquake and theft.

The Security Summit developed a plain language sample plan that tax pros can use for guidance in making their own WISP. The **sample plan** is available on IRS.gov.

A security plan should be appropriate to the company's size, scope of activities, complexity and the sensitivity of the customer data it handles.

Developing a WISP

A good **WISP** should identify the risks of data loss for the types of information handled by a company and focus on three areas:

1. Employee management and training.
2. Information systems.
3. Detecting and managing system failures.

Understanding post-breach responsibilities is important in creating a WISP. A good resource is the **FTC's Data Breach Response Guide.**

As a part of the plan, the FTC requires each firm to:

- Designate one or more employees to coordinate its information security program.
- Identify and assess the risks to customer information in each relevant area of the company's operation and evaluate the effectiveness of the current safeguards for controlling those risks.
- Design and implement a safeguards program, and regularly monitor and test it.
- Select service providers that can maintain appropriate safeguards.
- Evaluate and adjust the program considering relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

Maintaining a WISP

A good security plan requires regular maintenance and upkeep. Here are tips to keep a WISP effective:

- Once completed, tax professionals should keep their WISP in a format that others can easily read, such as PDF or Word. Making the WISP available to employees for training purposes is also encouraged. Storing a copy offsite or in the cloud is a recommended best practice in the event of a physical disaster.
- It is important to understand that a WISP is intended to be an evergreen document. It is important to regularly review and update any security plan, along with adjusting the plan to accommodate changes to the size, scope and complexity of a tax professional's business.
- As part of a security plan, the IRS also recommends tax professionals create a data theft response plan, which includes contacting their **IRS Stakeholder Liaison** to report a theft. Also see the **FTC data breach response requirements** listed above.

Publication 5709 (11-2022) Catalog Number 93463H Department of the Treasury **Internal Revenue Service** www.irs.gov

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

Publication 5708 (10-2022) Catalog Number 93462W Department of the Treasury **Internal Revenue Service www.irs.gov**

Table of Contents

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.

Requirements

The Gramm-Leach-Bliley Act (GLBA) is a U.S. law that requires financial institutions to protect customer data. In its implementation of the GLBA, the Federal Trade Commission (FTC) issued the Safeguards Rule to outline measures that are required to be in place to keep customer data safe. One requirement of the Safeguards Rule is implementing a WISP.

Under the GLBA, tax and accounting professionals are considered financial institutions, regardless of size. Financial institutions subject to the Safeguards Rule include mortgage brokers, real estate appraisers, universities, nonbank lenders, and check cashing businesses.

As a part of the plan, the FTC requires each firm to:

- Designate one or more employees to coordinate its information security program
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks
- Design and implement a safeguards program, and regularly monitor and test it
- Select service providers that can maintain appropriate safeguards by ensuring your contract requires them to maintain safeguards and oversee their handling of customer information
- Evaluate and adjust the program considering relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring

Getting Started on your WISP

Before you begin writing your WISP, take time to familiarize yourself with compliance requirements and your professional responsibilities. Some good resources to review before beginning include:

- **IRS Publication 4557**
- **FTC Data Breach Response Guide**

A security plan should be appropriate to the company's size, scope of activities, complexity, and the sensitivity of the customer data it handles. There is no one-size-fits-all WISP. For example, a sole practitioner can use a more abbreviated and simplified plan than a 10-partner accounting firm. A good WISP should focus on three areas:

- Employee management and training
- Information systems
- Detecting and managing system failures

It is a good idea to create an Employee/Contractor Acknowledgment of Understanding document for all personnel to keep a record of training and understanding of the policies in your WISP. Signing and dating training leaves a good documentation trail you can keep on file for several reasons – to show your adherence to the spirit of compliance and to have an enforceable accountability point in the event of a negligent employee. It is recommended that these acknowledgments be updated at annual training intervals and kept on file.

Once completed, keep your WISP in a format that others can easily read, such as PDF or Word. Making your WISP available to employees for training purposes is encouraged. Storing a copy offsite or in the cloud is a recommended best practice in the event of a physical disaster.

It is important to understand that a WISP is intended to be an evergreen document that is regularly reviewed and updated along with changes to the size, scope, and complexity of your business.

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

V. Document Safety Measures in place

a. Suggested policies to include in your WISP:
   - Data collection and retention
   - Data disclosure
   - Network protection
   - User access
   - Electronic data exchange
   - Wi-Fi access
   - Remote access
   - Connected devices
   - Reportable Incidents
b. Draft Employee Code of Conduct

VI. Draft an implementation clause

VII. Attachments

Sample Template

Written Information Security Plan (WISP)

For

[Your Firm Name Here]

This Document is for general distribution and is available to all employees.
This Document is available to Clients by request and with consent of the Firm's Data Security Coordinator.

Last Modified/Reviewed **[Last Modified Date]**
[Should review and update at least annually]

Written Information Security Plan (WISP)

I. OBJECTIVE

Our objective, in the development and implementation of this comprehensive **Written Information Security Plan (WISP)**, is to create effective administrative, technical, and physical safeguards for the protection of the **Personally Identifiable Information (PII)** retained by **[Your Firm Name],** (hereinafter known as **the Firm**). This WISP is to comply with obligations under the Gramm-Leach-Bliley Act and Federal Trade Commission Financial Privacy and Safeguards Rules to which the Firm is subject. The WISP sets forth our procedure for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII retained by the Firm. For purposes of this WISP, PII means information containing the first name and last name or first initial and last name of a Taxpayer, Spouse, Dependent, or Legal Guardianship person in combination with any of the following data elements retained by the Firm that relate to Clients, Business Entities, or Firm Employees:

- **A.** Social Security number, Date of Birth, or Employment data
- **B.** Driver's license number or state-issued identification card number
- **C.** Income data, Tax Filing data, Retirement Plan data, Asset Ownership data, Investment data
- **D.** Financial account number, credit or debit card number, with or without security code, access code, personal identification number; or password(s) that permit access to a client's financial accounts
- **E.** E-mail addresses, non-listed phone numbers, residential or mobile or contact information

PII shall not include information that is obtained from publicly available sources such as a Mailing Address or Phone Directory listing; or from federal, state or local government records lawfully made available to the general public.

II. PURPOSE

The purpose of the WISP is to:

- **A.** Ensure the Security and Confidentiality of all PII retained by the Firm.
- **B.** Protect PII against anticipated threats or hazards to the security or integrity of such information.
- **C.** Protect against any unauthorized access to or use of PII in a manner that creates a substantial risk of Identity Theft or Fraudulent or Harmful use.

III. SCOPE

The Scope of the WISP related to the Firm shall be limited to the following protocols:

- **A.** Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing PII.
- **B.** Assess the potential damage of these threats, taking into consideration the sensitivity of the PII.
- **C.** Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control identified risks.
- **D.** Design and implement this WISP to place safeguards to minimize those risks, consistent with the requirements of the Gramm-Leach-Bliley Act, the Federal Trade Commission Financial Privacy and Safeguards Rule, and National Institute of Standards recommendations.
- **E.** Regular monitoring and assessment of the effectiveness of aforementioned safeguards.

IV. IDENTIFIED RESPONSIBLE OFFICIALS

[The Firm] has designated [Employee's Name] to be the Data Security Coordinator (hereinafter the DSC). The DSC is the responsible official for the Firm data security processes and will implement, supervise, and maintain the WISP. Accordingly, the DSC will be responsible for the following:

- Implementing the WISP including all daily operational protocols
- Identifying all the Firm's repositories of data subject to the WISP protocols and designating them as Secured Assets with Restricted Access
- Verifying all employees have completed recurring Information Security Plan Training
- Monitoring and testing employee compliance with the plan's policies and procedures
- Evaluating the ability of any third-party service providers not directly involved with tax preparation and electronic transmission of tax returns to implement and maintain appropriate security measures for the PII to which we have permitted them access, and
- Requiring third-party service providers to implement and maintain appropriate security measures that comply with this WISP
- Reviewing the scope of the security measures in the WISP at least annually or whenever there is a material change in our business practices that affect the security or integrity of records containing PII
- Conducting an annual training session for all owners, managers, employees, and independent contractors, including temporary and contract employees who have access to PII enumerated in the elements of the WISP. All attendees at such training sessions are required to certify their attendance at the training and their familiarity with our requirements for ensuring the protection of PII. See Employee/Contractor Acknowledgement of Understanding at the end of this document

[The Firm] has designated [Employee's Name] to be the Public Information Officer (hereinafter PIO). The PIO will be the firm's designated public statement spokesperson. To prevent misunderstandings and hearsay, all outward-facing communications should be approved through this person who shall be in charge of the following:

- All client communications by phone conversation or in writing
- All statements to law enforcement agencies
- All releases to news media
- All information released to business associates, neighboring businesses, and trade associations to which the firm belongs

V. INSIDE THE FIRM RISK MITIGATION

To reduce internal risks to the security, confidentiality, and/or integrity of any retained electronic, paper, or other records containing PII, the Firm has implemented mandatory policies and procedures as follows:

PII Collection and Retention Policy

A. We will only collect the PII of clients, customers, or employees that is necessary to accomplish our legitimate business needs, while maintaining compliance with all federal, state, or local regulations.

B. Access to records containing PII is limited to employees whose duties, relevant to their job descriptions, constitute a legitimate need to access said records, and only for job-related purposes.

C. The DSC will identify and document the locations where PII may be stored on the Company premises:

- **a.** Servers, disk drives, solid-state drives, USB memory devices, removable media
- **b.** Filing cabinets, securable desk drawers, contracted document retention and storage firms
- **c.** PC Workstations, Laptop Computers, client portals, electronic Document Management
- **d.** Online (Web-based) applications, portals, and cloud software applications such as Box
- **e.** Database applications, such as Bookkeeping and Tax Software Programs
- **f.** Solid-state drives, and removable or swappable drives, and USB storage media

D. Designated written and electronic records containing PII shall be destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements.

- **a.** Paper-based records shall be securely destroyed by shredding or incineration at the end of their service life.
- **b.** Electronic records shall be securely destroyed by deleting and overwriting the file directory or by reformatting the drive on which they were housed.
- **c.** Specific business record retention policies and secure data destruction policies are in an attachment to this WISP.

Personnel Accountability Policy

A. A copy of the WISP will be distributed to all current employees and to new employees on the beginning dates of their employment. It will be the employee's responsibility to acknowledge in writing, by signing the attached sheet, that he/she received a copy of the WISP and will abide by its provisions. Employees are actively encouraged to advise the DSC of any activity or operation that poses risk to the secure retention of PII. If the DSC is the source of these risks, employees should advise any other Principal or the Business Owner.

- **a.** The Firm will create and establish general Rules of Behavior and Conduct regarding policies safeguarding PII according to IRS Pub. 4557 Guidelines. **[complete and attach after reviewing supporting NISTIR 7621, NIST SP-800 18, and Pub 4557 requirements]**
- **b.** The Firm will screen the procedures prior to granting new access to PII for existing employees.
- **c.** The Firm will conduct Background Checks on new employees who will have access to retained PII.
- **d.** The Firm may require non-disclosure agreements for employees who have access to the PII of any designated client determined to have highly sensitive data or security concerns related to their account.

B. The DSC or designated authorized representative will immediately train all existing employees on the detailed provisions of the Plan. All employees will be subject to periodic reviews by the DSC to ensure compliance.

C. All employees are responsible for maintaining the privacy and integrity of the Firm's retained PII. Any paper records containing PII are to be secured appropriately when not in use. Employees may not keep files containing PII open on their desks when they are not at their desks. Any computer file stored on the company network containing PII will be password-protected and/or encrypted. Computers must be locked from access when employees are not at their desks. At the end of the workday, all files and other records containing PII will be secured by employees in a manner that is consistent with the Plan's rules for protecting the security of PII.

D. Any employee who willfully discloses PII or fails to comply with these policies will face immediate disciplinary action that includes a verbal or written warning plus other actions up to and including termination of employment.

E. Terminated employees' computer access logins and passwords will be disabled at the time of termination. Physical access to any documents or resources containing PII will be immediately discontinued. Terminated employees will be required to surrender all keys, IDs or access codes or badges, and business cards that permit access to the firm's premises or information. Terminated employees' remote electronic access to personal information will be disabled; voicemail access, e-mail access, Internet access, Tax Software download/update access, accounts and passwords will be inactivated. The DSC or designee shall maintain a highly secured master list of all lock combinations, passwords, and keys, and will determine the need for changes to be made relevant to the terminated employee's access rights.

PII Disclosure Policy

A. No PII will be disclosed without authenticating the receiving party and without securing written authorization from the individual whose PII is contained in such disclosure. Access is restricted for areas in which personal information is stored, including file rooms, filing cabinets, desks, and computers with access to retained PII. An escort will accompany all visitors while within any restricted area of stored PII data.

B. The Firm will take all possible measures to ensure that employees are trained to keep all paper and electronic records containing PII securely on premises at all times. When there is a need to bring records containing PII offsite, only the minimum information necessary will be checked out. Records taken offsite will be returned to the secure storage location as soon as possible. Under no circumstances will documents, electronic devices, or digital media containing PII be left unattended in an employee's car, home, or in any other potentially insecure location.

C. All security measures included in this WISP shall be reviewed annually, beginning **[annual calendar review date]** to ensure that the policies contained in the WISP are adequate and meet all applicable federal and state regulations. Changes may be made to the WISP at any time they are warranted. When the WISP is amended, employees will be informed in writing. The DSC and principal owners of the firm will be responsible for the review and modification of the WISP, including any security improvement recommendations from employees, security consultants, IT contractors, and regulatory sources.

D. **[The Firm]** shares Employee PII in the form of employment records, pension and insurance information, and other information required of any employer. The Firm may share the PII of our clients with the state and federal tax authorities, Tax Software Vendor, a bookkeeping service, a payroll service, a CPA firm, an

Enrolled Agent, legal counsel, and/or business advisors in the normal course of business for any Tax Preparation firm. Law enforcement and governmental agencies may also have customer PII shared with them in order to protect our clients or in the event of a lawfully executed subpoena. An IT support company may occasionally see PII in the course of contracted services. Access to PII by these third-party organizations will be the minimum required to conduct business. Any third-party service provider that does require access to information must be compliant with the standards contained in this WISP at a minimum. The exceptions are tax software vendors and e-Filing transmitters; and the state and federal tax authorities, which are already compliant with laws that are stricter than this WISP requires. These additional requirements are outlined in IRS Publication 1345.

Reportable Event Policy

A. If there is a Data Security Incident that requires notifications under the provisions of regulatory laws such as The Gramm-Leach-Bliley Act, there will be a mandatory post-incident review by the DSC of the events and actions taken. The DSC will determine if any changes in operations are required to improve the security of retained PII for which the Firm is responsible. Records of and changes or amendments to the Information Security Plan will be tracked and kept on file as an addendum to this WISP.

B. The DSC is responsible for maintaining any Data Theft Liability Insurance, Cyber Theft Insurance Riders, or Legal Counsel on retainer as deemed prudent and necessary by the principal ownership of the Firm.

C. The DSC will also notify the IRS Stakeholder Liaison, and state and local Law Enforcement Authorities in the event of a Data Security Incident, coordinating all actions and responses taken by the Firm. The DSC or person designated by the coordinator shall be the sole point of contact with any outside organization not related to Law Enforcement, such as news media, non-client inquiries by other local firms or businesses and other inquirers.

VI. OUTSIDE THE FIRM RISK MITIGATION

To combat external risks from outside the firm network to the security, confidentiality, and/or integrity of electronic, paper, or other records containing PII, and improving - where necessary - the effectiveness of the current safeguards for limiting such risks, the Firm has implemented the following policies and procedures.

Network Protection Policy

A. Firewall protection, operating system security patches, and all software products shall be up to date and installed on any computer that accesses, stores, or processes PII data on the Firms network. This includes any Third-Party Devices connected to the network.

B. All system security software, including anti-virus, anti-malware, and internet security, shall be up to date and installed on any computer that stores or processes PII data or the Firms network.

C. Secure user authentication protocols will be in place to:

- **a.** Control username ID, passwords and Two-Factor Authentication processes
- **b.** Restrict access to currently active user accounts
- **c.** Require strong passwords in a manner that conforms to accepted security standards (using upper- and lower-case letters, numbers, and special characters, eight or more characters in length)
- **d.** Change all passwords at least every 90 days, or more often if conditions warrant
- **e.** Unique firm related passwords must not be used on other sites; or personal passwords used for firm business. Firm passwords will be for access to Firm resources only and not mixed with personal passwords

D. All computer systems will be continually monitored for unauthorized access or unauthorized use of PII data. Event Logging will remain enabled on all systems containing PII. Review of event logs by the DSC or IT partner will be scheduled at random intervals not to exceed 90 days.

E. The Firm will maintain a firewall between the internet and the internal private network. This firewall will be secured and maintained by the Firm's IT Service Provider. The Firewall will follow firmware/software updates per vendor recommendations for security patches. Workstations will also have a software-based firewall enabled.

F. Operating System (OS) patches and security updates will be reviewed and installed continuously. The DSC will conduct a top-down security review at least every 30 days.

Firm User Access Control Policy

A. The Firm will use 2-Factor Authentication (2FA) for remote login authentication via a cell phone text message, or an app, such as Google Authenticator or Duo, to ensure only authorized devices can gain remote access to the Firm's systems.

B. All users will have unique passwords to the computer network. The firm will not have any shared passwords or accounts to our computer systems, internet access, software vendor for product downloads, and so on. The passwords can be changed by the individual without disclosure of the password(s) to the DSC or any other Firm employee at any time.

C. Passwords will be refreshed every 90 days at a minimum and more often if conditions warrant. The DSC will notify employees when accelerated password reset is necessary.

D. If a Password Utility program, such as LastPass or Password Safe, is utilized, the DSC will first confirm that:

- **a.** Username and password information is stored on a secure encrypted site.
- **b.** 2-factor authentication of the user is enabled to authenticate new devices.

Electronic Exchange of PII Policy

A. It is Firm policy that PII will not be in any unprotected format, such as e-mailed in plain text, rich text, html, or other e-mail formats unless encryption or password protection is present. Passwords MUST be communicated to the receiving party via a method other than what is used to send the data; such as by phone call or SMS text message (out of stream from the data sent).

B. The Firm may use a Password Protected Portal to exchange documents containing PII upon approval of data security protocols by the DSC.

C. MS BitLocker or similar encryption will be used on interface drives, such as a USB drive, for files containing PII.

Wi-Fi Access Policy

A. Wireless access (Wi-Fi) points or nodes, if available, will use strong encryption. Firm Wi-Fi will require a password for access. If open Wi-Fi for clients is made available (guest Wi-Fi), it will be on a different network and Wi-Fi node from the Firm's Private work-related Wi-Fi.

B. All devices with wireless capability such as printers, all-in-one copiers and printers, fax machines, and smart devices such as TVs, refrigerators, and any other devices with Smart Technology will have default factory passwords changed to Firm-assigned passwords. All default passwords will be reset or the device will be disabled from wireless capability or the device will be replaced with a non-wireless capable device.

Remote Access Policy

The DSC and the Firm's IT contractor will approve use of Remote Access utilities for the entire Firm. **Remote access is dangerous if not configured correctly and is the preferred tool of many hackers.** Remote access using tools that encrypt both the traffic and the authentication requests (ID and Password) used will be the standard. Remote Access will not be available unless the Office is staffed and systems are monitored. **Nights and Weekends are high threat periods for Remote Access Takeover data theft.** Remote access will only be allowed using 2 Factor Authentication (2FA) in addition to username and password authentication.

Connected Devices Policy

A. Any new devices that connect to the Internal Network will undergo a thorough security review before they are added to the network. The Firm will ensure the devices meet all security patch standards and login and password protocols before they are connected to the network.

B. "AutoRun" features for USB ports and optical drives like CD and DVD drives on network computers and connected devices will be disabled to prevent malicious programs from self-installing on the Firm's systems.

C. The Firm or a certified third-party vendor will erase the hard drives or memory storage devices the Firm removes from the network at the end of their respective service lives. If any memory device is unable to be erased, it will be destroyed by removing its ability to be connected to any device, or circuitry will be shorted, or it will be physically rendered unable to produce any residual data still on the storage device.

D. The firm runs approved and licensed anti-virus software, which is updated on all servers continuously. Virus and malware definition updates are also updated as they are made available. The system is tested weekly to ensure the protection is current and up to date.

Information Security Training Policy

All employees will be trained on maintaining the privacy and confidentiality of the Firm's PII. The DSC will conduct training regarding the specifics of paper record handling, electronic record handling, and Firm security procedures at least annually. All new employees will be trained before PII access is granted, and periodic reviews or refreshers will be scheduled until all employees are of the same mindset regarding Information Security. Disciplinary action may be recommended for any employee who disregards these policies.

VII. IMPLEMENTATION

Effective **[date of implementation]**, [The Firm] has created this Written Information Security Plan (WISP) in compliance with regulatory rulings regarding implementation of a written data security plan found in the Gramm-Leach-Bliley Act and the Federal Trade Commission Financial Privacy and Safeguards Rules.

Signed: _____ Date: _____

Title: [Principal Operating Officer/Owner Title]

Signed: _____ Date: _____

Title: Data Security Coordinator

Added Detail for Consideration When Creating your WISP

Use this additional detail as you develop your written security plan. Review the description of each outline item and consider the examples as you write your unique plan.

Define the WISP objectives, purpose, and scope

Objective Statement: This defines the reason for the plan, stating any legal obligations such as compliance with the provisions of GLBA and sets the tone and defines the reasoning behind the plan. The Objective Statement should explain why the Firm developed the plan. It also serves to set the boundaries for what the document should address and why.

Purpose Statement: The Purpose Statement should explain **what** and **how** taxpayer information is being protected with the security process and procedures.

Scope Statement: The scope statement sets the **limits** on the **intent** and purpose of the WISP. Since you should not be legally held to a standard that was unforeseen at the writing or periodic updating of your WISP, you should set reasonable limits that the scope is intended to define.

Identify responsible individuals

Identify by name and position persons responsible for overseeing your security programs. Explain who will act in the roles of Data Security Coordinator (DSC) and Public Information Officer (PIO). In most firms of two or more practitioners, these should be different individuals. These roles will have concurrent duties in the event of a data security incident. Be sure to define the duties of each responsible individual.

- The Data Security Coordinator is the person tasked with the information security process, from securing the data while remediating the security weaknesses to training all firm personnel in security measures.
- The Public Information Officer is the “one voice” that speaks for the firm for client notifications and outward statements to third parties, such as local law enforcement agencies, news media, and local associates and businesses inquiring about their own risks.

Assess Risks

- Identify Risks: While building your WISP, take a close look at your business to identify risks of unauthorized access, use, or disclosure of information. Carefully consider your firm’s vulnerabilities.
- List types of information your office handles. Identifying the information your practice handles is a critical step in evaluating risk. Some types of information you may use in your firm includes taxpayer PII, employee records, and private business financial information. For example, do you handle paper and electronic documentation containing client or employee PII? List all types.
- List all potential types of loss (internal and external). Evaluate types of loss that could occur, including unauthorized access and disclosure and loss of access. Be sure to include any potential threats and vulnerabilities, such as theft, destruction, or accidental disclosure. Examples might include physical theft of paper or electronic files, electronic data theft due to Remote Access Takeover of your computer network, and loss due to fire, hurricane, tornado or other natural cause.
- Outline procedures to monitor your processes and test for new risks that may arise.

Inventory Hardware

- It is imperative to catalog all devices used in your practice that come in contact with taxpayer data. This could be anything from a computer, network devices, cell phones, printers, to modems and routers.
    - List description and physical location of each item
    - Record types of information stored or processed by each item

Example:

- Jane Doe Business Cell Phone, located with Jane Doe, processes emails from clients
- John Doe PC, located in John's office linked to the firms' network, processes tax returns, emails, company financial information.
- Network Router, located in the back storage room and is linked to office internet, processes all types of information

Sample Attachment E - Firm Hardware Inventory containing PII Data

Document Safety Measures

- This section sets the policies and business procedures the firm undertakes to secure all PII in the Firm's custody of clients, employees, contractors, governing any privacy-controlled physical (hard copy) data, electronic data, and handling by firm employees.

List policies for the following:

- Data collection and retention
    - Precisely define the minimal amount of PII the firm will collect and store
    - Define who shall have access to the stored PII data
    - Define where the PII data will be stored and in what formats
    - Designate when and which documents are to be destroyed and securely deleted after they have met their data retention life cycle
- **Data disclosure**
    - You should define any receiving party authentication process for PII received
    - Define how data containing PII will be secured while checked out of designated PII secure storage area
    - Determine any policies for the internet service provider, cloud hosting provider, and other services connected to any stored PII of the firm, such as 2 Factor Authentication requirements and compatibility
    - Spell out whom the Firm may share stored PII data with, in the ordinary course of business, and any requirements that these related businesses and agencies are compliant with the Firm's privacy standards
- **Network protection (List how your system and devices are protected)**
    - Firewall protection

- All security software, anti-virus, anti-malware, anti-tracker, and similar protections
- Secure user protocols
  - User IDs
  - Restricted access by job role
  - Password selection policy
  - Password controls to ensure no passwords are shared
  - Password change interval policy
  - Restriction on using firm passwords for personal use, and personal passwords for firm use
- Monitoring all computer systems for unauthorized access via event logs and routine event review
- Operating System patch and update policies by authorized personnel to ensure uniform security updates on all workstations

- **User access (How users access devices)**
  - Will your firm implement an Unsuccessful Login lockout procedure?
  - Two-Factor Authentication Policy controls
  - Determine any unique Individual user password policy
  - Approval and usage guidelines for any third-party password utility program
- **Remote access (How employees access data remotely)**
  - Set policy requiring 2FA for remote access connections.
  - Consider a no after-business-hours remote access policy. Historically, this is prime time for hackers, since the local networks they are hacking are not being monitored by employee users.
- **Connected devices (How new devices or software is added to the network)**
  - New network devices, computers, and servers must clear a security review for compatibility/ configuration
  - Configure access ports like USB ports to disable “autorun” features
  - Set policy on firm-approved anti-virus, anti-malware, and anti-tracking programs and require their use on every connected device.
  - Require any new software applications to be approved for use on the Firm’s network by the DSC or IT Professional prior to installation.
- **Reportable Incidents**

  Create both an Incident Response Plan & a Breach Notification Plan

  In the event of an incident, the presence of both a Response and a Notification Plan in your WISP reduces the unknowns of how to respond and should outline the necessary steps that each designated official must take to both address the issue and notify the required parties.
  - At a minimum, plans should include what steps will be taken to re-secure your devices, data, passwords, networks and who will carry out these actions

- Describe how the Firm Data Security Coordinator (DSC) will notify anyone assisting with a reportable data breach requiring remediation procedures
- Describe who will be responsible for maintaining any data theft liability insurance, Cyber Theft Rider policies, and legal counsel retainer if appropriate
- Describe the DSC duties to notify outside agencies, such as the IRS Stakeholder Liaison, Federal Trade Commission, State Attorney General, FBI local field office if a cybercrime, and local law enforcement agencies

- **Draft Employee Code of Conduct**

  Determine a personnel accountability policy including training guidelines for all employees and contractors, guidelines for behavior, and employee screening and background checks. Address any necessary non-disclosure agreements and privacy guidelines. Be sure to include information for terminated and separated employees, such as scrubbing access and passwords and ending physical access to your business.

Draft an Implementation Clause

When all appropriate policies and procedures have been identified and included in your plan, it is time for the final steps and implementation of your WISP. An Implementation clause should show the following elements:

- Date of implementation
- Firm Name
- That the plan is emplaced in compliance with the requirements of the GLBA
- That the plan is in compliance with the Federal Trade Commission Financial Privacy and Safeguards Rule
- Also add if additional state regulatory requirements apply
- The plan should be signed by the principal operating officer or owner, and the DSC and dated the date of implementation

Ancillary Attachments

Attach any ancillary procedures as attachments. These are the specific task procedures that support firm policies, or business operation rules. For example, a separate Records Retention Policy makes sense. If regulatory records retention standards change, you update the attached procedure, not the entire WISP. Other potential attachments are Rules of Behavior and Conduct Safeguarding Client PII, as recommended in Pub 4557. Another good attachment would be a Security Breach Notifications Procedure.

Sample Attachment A - Record Retention Policy

Determine the firm's procedures on storing records containing any PII.

- How long will you keep historical data records, different firms have different standards? There are some Federal and state guidelines for records retention periods.
- How will you destroy records once they age out of the retention period?
  - How will paper records are to be stored and destroyed at the end of their service life
  - How will electronic records be stored, backed up, or destroyed at the end of their service life

Best Practice: *Keeping records longer than the minimum record retention period can put clients at some additional risk for deeper audits. By common discovery rules, if the records are there, they can be audited back as far as the statutes of limitations will allow. Promptly destroying old records at the minimum required timeframe will limit any audit or other legal inquiry into your clients' records to that time frame only.*

Sample Attachment B - Rules of Behavior and Conduct Safeguarding Client PII

Having some rules of conduct in writing is a very good idea. It standardizes the way you handle and process information for everyone in the firm. This attachment can be reproduced and posted in the breakroom, at desks, and as a guide for new hires and temporary employees to follow as they get oriented to safe data handling procedures. These sample guidelines are loosely based on the National Institute of Standards guidelines and have been customized to fit the context of a Tax & Accounting Firm's daily operations.

Best Practice: *At the beginning of a new tax season cycle, this addendum would make good material for a monthly security staff meeting. Keeping security practices top of mind is of great importance. Other monthly topics could include how phishing emails work, phone call grooming by a bad actor, etc. SANS.ORG has great resources for security topics. The Ouch! Newsletter can be used as topical material for your Security meetings.*

Sample Attachment C - Security Breach Procedures and Notifications

It is a good idea to have a guideline to follow in the immediate aftermath of a data breach. To be prepared for the eventuality, you must have a procedural guide to follow. This attachment will need to be updated annually for accuracy. Subscribing to IRS e-news and topics like the Protect Your Clients, Protect Yourselves series will inform you of changes as fraud prevention procedures mature over time.

Sample Attachment D - Employee/Contractor Acknowledgement of Understanding

It is a good idea to have a signed acknowledgment of understanding. This is particularly true when you hire new or temporary employees, and when you bring a vendor partner into your business circle, such as your IT Pro, cleaning service, or copier servicing company. They need to know you handle sensitive personal data and you take the protection of that data very seriously.

Best Practice: *It is important that employees see the owners and managers put themselves under the same rules as everyone else. When you roll out your WISP, placing the signed copies in a collection box on the office manager's desk for a time for anyone to see, for example, is a good way for everyone to see that all employees are accountable. Placing the Owners and Data Security Coordinator's signed copy on the top of the stack prominently shows you will play no favorites and are all pledging to the same standard of conduct. This acknowledgement process should be refreshed annually after an annual meeting discussing the Written Information Security Plan and any operational changes made from the prior year.*

Sample Attachment E - Firm Hardware Inventory containing PII Data

Keeping track of data is a challenge. A good way to make sure you know where everything is and when it was put in service or taken out of service is recommended. This is especially true of electronic data.

- Include paper records by listing filing cabinets, dated archive storage boxes, and any alternate locations of storage that may be off premises.
- List all desktop computers, laptops, and business-related cell phones which may contain client PII.
- List storage devices, removable hard drives, cloud storage, or USB memory sticks containing client PII.

Best Practice: *Set a policy that no client PII can be stored on any personal employee devices such as personal (not firm owned) memory sticks, home computers, and cell phones that are not under the direct control of the firm. This ensures all devices meet the security standards of the firm, such as having any auto-run features turned off, and they are standardized for virus and malware scans.*

Sample Attachment F - Firm Employees Authorized to Access PII

Having a list of employees and vendors, such as your IT Pro, who are authorized to handle client PII is a good idea. You should not allow someone who may not fully understand the seriousness of the secure environment your firm operates in to access privacy-controlled information. Additionally, an authorized access list is a good place to start the process of removing access rights when a person retires or leaves the firm. Having a systematic process for closing down user rights is just as important as granting them.

- List name, job role, duties, access level, date access granted, and date access Terminated
- Be sure to include contractors, such as your IT professionals, hosting vendors, and cleaning and housekeeping, who have access to any stored PII in your safekeeping, physical or electronic.
- List any other data access criteria you wish to track in the event of any legal or law enforcement request due to a data breach inquiry. Examples:
    - John Smith - Office Manager / Day-to-Day Operations / Access all digital and paper-based data / Granted January 2, 2018
    - Jane Robinson - Senior Tax Partner / Tax Planning and Preparation / Access all digital and paper-based data / Granted December 01, 2015
    - Jill Johnson - Receptionist / Phones/Scheduling / Access ABC scheduling software / Granted January 10, 2020 / Terminated December 31, 2020
    - Jill Johnson - Tax Preparer / 1040 Tax Preparation / Access all digital and paper-based data / Granted January 2, 2021

Best Practice: *If a person has their rights increased or decreased It is a good idea to terminate the old access rights on one line, and then add a new entry for the new access rights granted. This shows a good chain of custody for rights and shows a progression. For the same reason, it is a good idea to show a person who goes into semi-retirement and has less rights than before and the date the status changed.*

Sample Attachment A: Record Retention Policies

Designated retained written and electronic records containing PII will be destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements.

It is Firm policy to retain no PII records longer than required by current regulations, practices, or standards.

I. In no case shall paper or electronic retained records containing PII be kept longer than _____ Years.

II. Paper-based records shall be securely destroyed by cross-cut shredding or incineration at the end of their service life.

III. Electronic records shall be securely destroyed by deleting and overwriting the file directory or by reformatting the drive where they were housed or destroying the drive disks rendering them inoperable if they have reached the end of their service life.

Sample Attachment B: Rules of Behavior and Conduct Safeguarding Client PII

Create and distribute rules of behavior that describe responsibilities and expected behavior regarding computer information systems as well as paper records and usage of taxpayer data. Have all information system users complete, sign, and comply with the rules of behavior. **NISTIR 7621, Small Business Information Security: The Fundamentals, Section 4**, has information regarding general rules of Behavior, such as:

- **Be careful of email attachments and web links**
    - Do not click on a link or open an attachment that you were not expecting. If it appears important, call the sender to verify they sent the email and ask them to describe what the attachment or link is. Before you click a link (in an email or on social media, instant messages, other webpages), hover over that link to see the actual web address it will take you to. Train employees to recognize phishing attempts and who to notify when one occurs.
- **Use separate personal and business computers, mobile devices, and email accounts**
    - This is especially important if other people, such as children, use personal devices. Do not conduct business or any sensitive activities (like online business banking) on a personal computer or device and do not engage in activities such as web surfing, gaming, downloading videos, etc., on business computers or devices. Do not send sensitive business information to personal email addresses.
- **Do not connect personal or untrusted storage devices or hardware into computers, mobile devices, or networks.**
    - Do not share USB drives or external hard drives between personal and business computers or devices. Do not connect any unknown/untrusted hardware into the system or network, and do not insert any unknown CD, DVD, or USB drive. Disable the “AutoRun” feature for the USB ports and optical drives like CD and DVD drives on business computers to help prevent such malicious programs from installing on the systems.
- **Be careful downloading software**
    - Do not download software from an unknown web page. Be very careful with freeware or shareware.
- **Watch out when providing personal or business information**
    - Social engineering is an attempt to obtain physical or electronic access to information by manipulating people. A very common type of attack involves a person, website, or email that pretends to be something it’s not. A social engineer will research a business to learn names, titles, responsibilities, and any personal information they can find; calls or sends an email with a believable but made-up story designed to convince you to give certain information.
    - Never respond to unsolicited phone calls that ask for sensitive personal or business information. Employees should notify their management whenever there is an attempt or request for sensitive business information.
    - Never give out usernames or passwords. No company should ask for this information for any reason. Also, beware of people asking what kind of operating system, brand of firewall, internet browser, or what applications are installed. This is information that can make it easier for a hacker to break into the system.

- **Watch for harmful pop-ups**
    - When connected to and using the Internet, do not respond to popup windows requesting that users click “OK.” Use a popup blocker and only allow popups on trusted websites.
- **Use strong passwords**
    - Good passwords consist of a random sequence of letters (upper- and lower-case), numbers, and special characters. The NIST recommends passwords be at least 12 characters long. For systems or applications that have important information, use multiple forms of identification (called “multi-factor” or “dual factor” authentication).
    - Many devices come with default administration passwords – these should be changed immediately when installing and regularly thereafter. Default passwords are easily found or known by hackers and can be used to access the device. The product manual or those who install the system should be able to show you how to change them.
    - Passwords should be changed at least every three months.
    - Passwords to devices and applications that deal with business information should not be re-used.
    - You may want to consider using a password management application to store your passwords for you.
- **Conduct online business more securely**
    - Online business/commerce/banking should only be done using a secure browser connection. This will normally be indicated by a small lock visible in the lower right corner or upper left of the web browser window.
    - Erase the web browser cache, temporary internet files, cookies, and history regularly. Ensure to erase this data after using any public computer and after any online commerce or banking session. This prevents important information from being stolen if the system is compromised. This will also help the system run faster. Typically, this is done in the web browser’s “privacy” or “security” menu. Review the web browser’s help manual for guidance.

Sample Attachment C: Security Breach Procedures and Notifications

I. Notifications

If the Data Security Coordinator determines that PII has been stolen or lost, the Firm will notify the following entities, describing the theft or loss in detail, and work with authorities to investigate the issue and to protect the victim's identity and credit.

- The **IRS Stakeholder Liaison** who coordinates IRS divisions and other agencies regarding a Tax Professional Office data breach.
- The state Attorney General's Office
- The FBI if it is a cyber-crime involving electronic data theft
- The Federal Trade Commission, in accordance with GLB Act provisions as outlined in the Safeguards Rule.
- Local law enforcement
- Tax software vendor (can assist with next steps after a data breach incident)
- Liability insurance carrier who may provide forensic IT services
- Legal counsel
- To the extent required by regulatory laws and good business practices, the Firm will also notify the victims of the theft so that they can protect their credit and identity. The FTC provides guidance for identity theft notifications in: **Information Compromise and the Risk of Identity Theft: Guidance for Your Business**

II. Procedures

Read this **IRS Newswire Alert** for more information

Examples:

- Go to IRS e-Services and check your EFIN activity report to see if more returns have been filed on your EFIN than you transmitted.
- Check to see if you can tell if the returns in question were submitted at odd hours that are not during normal hours of operation, such as overnight or on weekends.
- Were the returns transmitted on a Monday or Tuesday morning?
    - Typically, a thief will remotely steal the client data over the weekend when no one is in the office to notice. They then rework the returns over the weekend and transmit them on a normal business workday just after the weekend.

Sample Attachment D: Employee/Contractor Acknowledgement of Understanding

I, **[Employee Name]**, do hereby acknowledge that I have been informed of the Written Information Security Plan used by [The Firm]. I have undergone training conducted by the Data Security Coordinator. I have also been able to have all questions regarding procedures answered to my satisfaction so that I fully understand the importance of maintaining strict compliance with the purpose and intent of this WISP.

I also understand that there will be periodic updates and training if these policies and procedures change for any reason. It has been explained to me that non-compliance with the WISP policies may result in disciplinary actions up to and including termination of employment.

I understand the importance of protecting the Personally Identifiable Information of our clients, employees, and contacts, and will diligently monitor my actions, as well as the actions of others, so that [The Firm] is a safe repository for all personally sensitive data necessary for business needs.

Signed,

[Employee Name] Date: **[Date of Initial/Last Training]**

Title: **[Employee Title Description]**

Sample Attachment E: Firm Hardware Inventory containing PII Data

Below is the enumerated list of hardware and software containing client or employee PII that will be periodically audited for compliance with this WISP.

Hardware Item	Location	Principal User	In-Service Date	Last Inventoried

Sample Attachment F: Firm Employees Authorized to Access PII

Name	Role	Job Duties	Access Level	Date access Granted	Date Access Terminated
John Doe	DSC	Office Manager	Full access to all PII	01/01/2015	

Reference A. The Glossary of Terms

Anti-virus software - software designed to detect and potentially eliminate viruses before damaging the system. Can also repair or quarantine files that have already been infected by virus activity.

Attachment - a file that has been added to an email. It could be something useful to you, or something harmful to your computer.

Authentication - confirms the correctness of the claimed identity of an individual user, machine, software component or any other entity.

Breach - unauthorized access of a computer or network, usually through the electronic gathering of login credentials of an approved user on the system.

Clear desk Policy - a policy that directs all personnel to clear their desks at the end of each working day, and file everything appropriately. Desks should be cleared of all documents and papers, including the contents of the "in" and "out" trays - not simply for cleanliness, but also to ensure that sensitive papers and documents are not exposed to unauthorized persons outside of working hours.

Clear screen Policy - a policy that directs all computer users to ensure that the contents of the screen are protected from prying eyes and opportunistic breaches of confidentiality. Typically, the easiest means of compliance is to use a screensaver that engages either on request or after a specified brief period.

Cybersecurity - the protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems.

Data Security Coordinator (DSC) - the firm-designated employee who will act as the chief data security officer for the firm. The DSC is responsible for all aspects of your firm's data security posture, especially as it relates to the PII of any client or employee the firm possesses in the course of normal business operations.

Data breach - an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

Encryption - a data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that it appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using a decryption key.

Firewall - a hardware or software link in a network that inspects all data packets coming and going from a computer, permitting only those that are authorized to reach the other side. It is helpful in controlling external access to a computer or network.

GLBA - Gramm-Leach-Bliley Act. Administered by the Federal Trade Commission. Establishes safeguards for all privacy-controlled information through business segment Safeguards Rule enforced business practices.

Hardware firewall - a dedicated computer configured to exclusively provide firewall services between another computer or network and the internet or other external connections.

Malware - (malicious software) any computer program designed to infiltrate, damage or disable computers.

Network - two or more computers that are grouped together to share information, software, and hardware. Can be a local office network or an internet-connection based network.

Out-of-stream - usually relates to the forwarding of a password for a file via a different mode of communication separate from the protected file. Example: Password protected file was emailed, the password was relayed to the recipient via text message, outside of the same stream of information from the protected file.

Patch - a small security update released by a software manufacturer to fix bugs in existing programs.

Phishing email - broad term for email scams that appear legitimate for the purpose of tricking the recipient into sharing sensitive information or installing malware.

PII - Personally Identifiable Information. The name, address, SSN, banking or other information used to establish official business. Also known as Privacy-Controlled Information.

Public Information Officer (PIO) - the PIO is the single point of contact for any outward communications from the firm related to a data breach incident where PII has been exposed to an unauthorized party. This position allows the firm to communicate to affected clients, media, or local businesses and associates in a controlled manner while allowing the Data Security Coordinator freedom to work on remediation internally.

Risk analysis - a process by which frequency and magnitude of IT risk scenarios are estimated; the initial steps of risk management; analyzing the value of assets to the business, identifying threats to those assets and evaluating how vulnerable each asset is to those threats.

Security awareness - the extent to which every employee with access to confidential information understands their responsibility to protect the physical and information assets of the organization.

Service providers - any business service provider contracted with for services, such as janitorial services, IT Professionals, and document destruction services employed by the firm who may come in contact with sensitive client PII.

Software firewall - an application installed on an existing operating system that adds firewall services to the existing programs and services on the system.

VPN (Virtual Private Network) - a secure remote network or Internet connection encrypting communications between a local device and a remote trusted device or service that prevents en-route interception of data.

Written Information Security Plan -a documented, structured approach identifying related activities and procedures that maintain a security awareness culture and to formulate security posture guidelines. Mandated for Tax & Accounting firms through the FTC Safeguards Rule supporting the Gramm-Leach-Bliley Act privacy law.

Resource Links:

Below are helpful links from within the WISP creation guide above and also from outside sources like the Federal Communications Commission (FCC), and the National Institute of Standards and Technology (NIST). These resources in addition to IRS and Federal Trade Commission resources will support your efforts to create a durable Written Information Security Plan for your firm.

Federal Trade Commission

- **FTC Financial Institution How to Comply**
- **FTC Safeguards Rule**
- **FTC Data Breach Response Guide**

National Institute of Standards

- Cybercrime & Cyber Threats to Small Business
    - **Cybercrime its worse we thought**
    - **Cybercrime existential threat small business**
- **NIST Computer Security Resource Center**
- **NIST Cybersecurity Framework examples**

Federal Communications Commission

- **FCC Cyber Threat Resources**

Internal Revenue Service

- **IRS Publication 4557**
- **IRS Stakeholder Liaison**
- **IRS Data Theft Reporting Process**

Identity Protection PIN

Opt-In Program for Taxpayers

WHAT'S NEW **You are now eligible to voluntarily get an Identity Protection PIN that will help protect you from tax-related identity theft.**

What is the IP PIN?

The IP PIN is a 6-digit number assigned to eligible taxpayers. It helps prevent identity thieves from filing fraudulent tax returns with stolen Social Security numbers (SSNs). An IP PIN helps the IRS verify taxpayers' identities and accept their electronic or paper tax returns for processing. The IRS issues IP PINs to confirmed identity theft victims once their cases are resolved. This process is unchanged. What is new is that any taxpayers who wants an IP PIN, even if they are not victims of identity theft, may now obtain one.

About the IP PIN Opt-in Program

Here's what you need to know before applying for your IP PIN:

- This is a voluntary program.
- You must pass a rigorous identity verification process.
- Spouses and dependents are eligible for an IP PIN if they can verify their identities.
- An IP PIN is valid for a calendar year.
- A new IP PIN is generated each filing season, which you must obtain using the online tool.
- The IP PIN tool is unavailable generally mid-November through mid-January each year.
- Correct IP PINs must be entered on electronic and paper tax returns to avoid rejections and delays.

How to Get an IP PIN

The fastest, easiest and preferred way is by using the Get an IP PIN online tool. Here's how it works:

- Go to **IRS.gov/IPPIN**, select the Get an IP PIN tool, verify your identity and create an account
- Your IP PIN will be revealed to you.

Can't pass online identity proofing?

There are alternatives but there will be a delay in obtaining an IP PIN. Here's how it works:

- File Form 15227 if you have a valid SSN or ITIN, the adjusted gross income on your last filed return is below $73,000 for Individuals or $146,000 for Married Filing Joint, and access to a telephone. An IRS assistor will call you, validate your identity and ensure that you receive an IP PIN the next filing season.
- If you are ineligible for Form 15227, you may schedule a visit at a Taxpayer Assistance Center to request an IP PIN. You can find the TAC office closest to you with our **Taxpayer Assistance Locator tool** or call (844-545-5640) to schedule an appointment.

IMPORTANT: The IRS will never email, text or call you to request your IP PIN. Do not reveal your IP PIN to anyone but your trusted tax software provider or tax preparer. Neither your provider nor preparer will ask for your IP PIN except to complete your tax return. Protect your IP PIN from theft, especially scams.

www.irs.gov/securitysummit

Protect personal and financial information online

The IRS and Security Summit partners remind people to take these basic steps when shopping online:

- ***Use security software for computers and mobile phones – and keep it updated.***
- ***Make sure anti-virus software for computers has a feature to stop malware, and that there is a firewall enabled that can prevent intrusions.***
- ***Use strong and unique passwords for all accounts.***
- ***Use multi-factor authentication whenever possible.***
- ***Shop only secure websites by looking for the "https" in web addresses and the padlock icon.***
- ***Avoid shopping on unsecured and public Wi-Fi in places such as coffee shops, malls or restaurants.***

Publication 5461 (Rev.11-2022) Catalog Number 75057B Department of the Treasury **Internal Revenue Service** www.irs.gov

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

Most cyberattacks are aimed at small businesses with fewer than 100 employees.

Here are some reminders:

- ***Learn about best security practices for small businesses.***
- ***IRS continues protective masking of sensitive information on business transcripts.***
- ***A Business Identity Theft Affidavit, Form 14039-B, is available for businesses to report theft to the IRS.***
- ***Beware of various scams, especially the W-2 scam that attempts to steal employee income information.***
- ***Check out the "Business" section on IRS's Identity Theft Central at IRS.gov/IdentityTheft.***

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

IRS advises that improperly forgiven Paycheck Protection Program loans are taxable

IR-2022-162, Sept. 21, 2022

WASHINGTON – The Internal Revenue Service recently issued guidance addressing improper forgiveness of a Paycheck Protection Program loan (PPP loan).

The guidance confirms that, when a taxpayer's loan is forgiven based upon misrepresentations or omissions, the taxpayer is not eligible to exclude the forgiveness from income and must include in income the portion of the loan proceeds that were forgiven based upon misrepresentations or omissions. Taxpayers who inappropriately received forgiveness of their PPP loans are encouraged to take steps to come into compliance by, for example, filing amended returns that include forgiven loan proceed amounts in income.

"This action underscores the Internal Revenue Service's commitment to ensuring that all taxpayers are paying their fair share of taxes," said IRS Commissioner Chuck Rettig. "We want to make sure that those who are abusing such programs are held accountable, and we will be considering all available treatment and penalty streams to address the abuses."

Many PPP loan recipients who received loan forgiveness were qualified and used the loan proceeds properly to pay eligible expenses. However, the IRS has discovered that some recipients who received loan forgiveness did not meet one or more eligibility conditions. These recipients received forgiveness of their PPP loan through misrepresentation or omission and either did not qualify to receive a PPP loan or misused the loan proceeds.

The PPP loan program was established by the Coronavirus Aid, Relief and Economic Security Act (CARES Act) to assist small US businesses that were adversely affected by the COVID-19 pandemic in paying certain expenses. The PPP loan program was further extended by the Economic Aid to Hard-Hit Small Businesses, Nonprofits and Venues Act.

Under the terms of the PPP loan program, lenders can forgive the full amount of the loan if the loan recipient meets three conditions.

1 - The loan recipient was eligible to receive the PPP loan. An eligible loan recipient:

- is a small business concern, independent contractor, eligible self-employed individual, sole proprietor, business concern, or a certain type of tax-exempt entity;
- was in business on or before February 15, 2020; and
- had employees or independent contractors who were paid for their services, or was a self-employed individual, sole proprietor or independent contractor.

2 - The loan proceeds had to be used to pay eligible expenses, such as payroll costs, rent, interest on the business' mortgage, and utilities.

3 - The loan recipient had to apply for loan forgiveness. The loan forgiveness application required a loan recipient to attest to eligibility, verify certain financial information, and meet other legal qualifications.

If the 3 conditions above are met, then under the PPP loan program the forgiven portion is excluded from income. If the conditions are not met, then the amount of the loan proceeds that were forgiven but do not meet the conditions must be included in income and any additional income tax must be paid.

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

To report tax-related illegal activities relating to PPP loans, submit Form 3949-A, Information Referral. You should also report instances of IRS-related phishing attempts and fraud to the Treasury Inspector General for Tax Administration at 800-366-4484.

-30-

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Employers warned to beware of third parties promoting improper Employee Retention Credit claims

IR-2022-183, Oct. 19, 2022

WASHINGTON -- The Internal Revenue Service today warned employers to be wary of third parties who are advising them to claim the Employee Retention Credit (ERC) when they may not qualify. Some third parties are taking improper positions related to taxpayer eligibility for and computation of the credit.

These third parties often charge large upfront fees or a fee that is contingent on the amount of the refund and may not inform taxpayers that wage deductions claimed on the business' federal income tax return must be reduced by the amount of the credit.

If the business filed an income tax return deducting qualified wages before it filed an employment tax return claiming the credit, the business should file an amended income tax return to correct any overstated wage deduction.

Businesses are encouraged to be cautious of advertised schemes and direct solicitations promising tax savings that are too good to be true. Taxpayers are always responsible for the information reported on their tax returns. Improperly claiming the ERC could result in taxpayers being required to repay the credit along with penalties and interest.

What is the ERC?

The ERC is a refundable tax credit designed for businesses who continued paying employees while shutdown due to the COVID-19 pandemic or had significant declines in gross receipts from March 13, 2020, to Dec. 31, 2021. Eligible taxpayers can claim the ERC on an original or amended employment tax return for a period within those dates.

To be eligible for the ERC, employers must have:

- sustained a full or partial suspension of operations due to orders from an appropriate governmental authority limiting commerce, travel, or group meetings due to COVID-19 during 2020 or the first three quarters of 2021,
- experienced a significant decline in gross receipts during 2020 or a decline in gross receipts during the first three quarters of 2021, or
- qualified as a recovery startup business for the third or fourth quarters of 2021.

As a reminder, only recovery startup businesses are eligible for the ERC in the fourth quarter of 2021. Additionally, for any quarter, eligible employers cannot claim the ERC on wages that were reported as payroll costs in obtaining PPP loan forgiveness or that were used to claim certain other tax credits.

To report tax-related illegal activities relating to ERC claims, submit Form 3949-A, Information Referral. You should also report instances of fraud and IRS-related phishing attempts to the Treasury Inspector General for Tax Administration at 800-366-4484.

Go to IRS.gov to learn more about eligibility requirements and how to claim the Employee Retention Credit :

- For qualified wages paid after March 12, 2020, and before Jan. 1, 2021 – Notice 2021-20, Notice 2021-49, and Revenue Procedure 2021-33
- For qualified wages paid after Dec. 31, 2020, and before July 1, 2021 – Notice 2021-23, Notice 2021-49 and Revenue Procedure 2021-33
- For qualified wages paid after June 30, 2021, and before Oct. 1, 2021 – Notice 2021-49 and Revenue Procedure 2021-33

- For qualified wages paid after Sept. 30, 2021, and before Jan. 1, 2022 – Notice 2021-49 and Notice 2021-65

Additional Information

- Employee Retention Credit - 2020 vs 2021 Comparison Chart | Internal Revenue Service (irs.gov)
- Form 941-X Instructions (April 2022 Revision) – for use in conjunction with Form 941 Instructions from relevant calendar quarter
- Form 941 Instructions (December 2021 Revision)
- Form 941 Instructions (2020 Revisions)
- Form 943, 943-X, 944, 944-X, CT-1 and CT-1-X Instructions

— 30 —

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

IRS expands voice bot options for faster service, less wait time

Assistance for eligible taxpayers in setting up or modifying payment plans now available; more functions planned in 2022 to help taxpayers obtain account information

Voice Bot Video

IR-2022-127, June 17, 2022

WASHINGTON – The Internal Revenue Service today announced expanded voice bot options to help eligible taxpayers easily verify their identity to set up or modify a payment plan while avoiding long wait times.

"This is part of a wider effort at the IRS to help improve the experience of taxpayers," said IRS Commissioner Chuck Rettig. "We continue to look for ways to better assist taxpayers, and that includes helping people avoid waiting on hold or having to make a second phone call to get what they need. The expanded voice bots are another example of how technology can help the IRS provide better service to taxpayers."

Voice bots run on software powered by artificial intelligence, which enables a caller to navigate an interactive voice response. The IRS has been using voice bots on numerous toll-free lines since January, enabling taxpayers with simple payment or notice questions to get what they need quickly and avoid waiting. Taxpayers can always speak with an English- or Spanish-speaking IRS telephone representative if needed.

Eligible taxpayers who call the Automated Collection System (ACS) and Accounts Management toll-free lines and want to discuss payment plan options can authenticate or verify their identities through a personal identification number (PIN) creation process. Setting up a PIN is easy: Taxpayers will need their most recent IRS bill and some basic personal information to complete the process.

"To date, the voice bots have answered over 3 million calls. As we add more functions for taxpayers to resolve their issues, I anticipate many more taxpayers getting the service they need quickly and easily," said Darren Guillot, IRS Deputy Commissioner of Small Business/Self Employed Collection & Operations Support.

Additional voice bot service enhancements are planned in 2022 that will allow authenticated individuals (taxpayers with established or newly created PINs) to get:

- Account and return transcripts.
- Payment history.
- Current balance owed.

In addition to the payment lines, voice bots help people who call the Economic Impact Payment (EIP) toll-free line with general procedural responses to frequently asked questions. The IRS also added voice bots for the Advance Child Tax Credit toll-free line in February to provide similar assistance to callers who need help reconciling the credits on their 2021 tax return.

The IRS also reminds taxpayers about numerous other available self-service options.

-30-

IRS.gov/payments

Expanded IRS voice bot options help taxpayers set up or modify a payment plan

The IRS began using English and Spanish voice bots on some of its toll-free help lines in January 2022. Since then, IRS is continuing to add voice bots to additional toll-free lines, while also expanding what these voice bots can do to help taxpayers.

The newest feature available, for those who are eligible, is to use the voice bot to set up or change a payment plan, while avoiding wait times.

Taxpayer: ***I have a question about an installment agreement.***

Voice bot: ***Sure, I can help you with a payment plan. To use this feature, a taxpayer must be able to authenticate their identity.***

- If a taxpayer received a bill from the IRS, they'll need that bill and a few pieces of basic information to set up a PIN and authenticate their identity.
- They should keep track of their PIN because it can be used again in the future.
- Their payment plan options may include a short-term plan or a long-term plan, also known as an installment agreement.

If a taxpayer has a current payment plan, they may be able to make changes, including updating payment amounts and/or changing payment dates.

If a taxpayer can't resolve their issue through the voice bot, they can ask to speak with an IRS phone assistor.

Taxpayer: ***Can I speak to a customer service agent please?***

Voice bot: ***Please hold while I transfer you to a representative.***

The IRS also has other self-service options available on IRS.gov.

For more information, check out IRS.gov/payments.

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

IRS: Taxpayers now have more options to correct, amend returns electronically

IR-2022-130, June 23, 2022

WASHINGTON — The Internal Revenue Service announced today that more forms can now be amended electronically. These include people filing corrections to the Form 1040-NR, U.S. Nonresident Alien Income Tax Return and Forms 1040-SS, U.S. Self-Employment Tax Return (Including the Additional Child Tax Credit for Bona Fide Residents of Puerto Rico) and Forms 1040-PR, Self-Employment Tax Return – Puerto Rico.

“This initiative has come a long way from 2020 when we first launched the ability to file amended returns, which was an important milestone to help taxpayers and the tax community," said IRS Commissioner Chuck Rettig. "This new feature will further help people needing to make corrections. This development will also assist the IRS with its inventory work on the current backlog of amended returns. This is another tool we’re using to help get us back on track.”

Additionally, a new, electronic checkbox has been added for Forms 1040/1040-SR, 1040-NR and 1040-SS/1040-PR to indicate that a superseding return is being filed electronically. A superseded return is one that is filed after the originally filed return but submitted before the due date, including extensions. Taxpayers can also amend their return electronically if there is change to their filing status or to add a dependent who was previously claimed on another return.

About 3 million Forms 1040-X are filed by taxpayers each year. Taxpayers can still use the "Where's My Amended Return?" online tool to check the status of their electronically-filed Form 1040-X.

Forms 1040, 1040-NR and 1040-SR can still be amended electronically for tax years 2019, 2020 and 2021 along with corrected Forms 1040-SS and Form 1040-PR for tax year 2021.

In general, taxpayers still have the option to submit a paper version of the Form 1040-X and should follow the instructions for preparing and submitting the paper form.

The IRS continues to look at this important area, and more enhancements are planned for the future.

-30-

An Overview of the IRS's 2022 "Dirty Dozen" Tax Scams

Compiled annually, the Dirty Dozen lists a variety of common scams that taxpayers can encounter anytime. The IRS warns taxpayers, tax professionals and financial institutions to beware of these scams. This year's list is divided into five groups. Here's an overview of the top twelve tax scams of 2022.

Potentially abusive arrangements

The 2022 Dirty Dozen begins with four transactions that are wrongfully promoted and will likely attract additional agency compliance efforts in the future. Those four abusive transactions involve charitable remainder annuity trusts, Maltese individual retirement arrangements, foreign captive insurance, and monetized installment sales.

Pandemic-related scams

This IRS reminds taxpayers that criminals still use the COVID-19 pandemic to steal people's money and identity with phishing emails, social media posts, phone calls, and text messages.

All these efforts can lead to sensitive personal information being stolen, and scammers using this to try filing a fraudulent tax return as well as harming victims in other ways. Some of the scams people should continue to be on the lookout for include Economic Impact Payment and tax refund scams, uunemployment fraud leading to inaccurate taxpayer 1099-Gs, fake employment offers on social media, and fake charities that steal taxpayers' money.

Offer in Compromise "mills"

Offer in Compromise or OIC "mills," make outlandish claims, usually in local advertising, about how they can settle a person's tax debt for pennies on the dollar. Often, the reality is that taxpayers pay the OIC mill a fee to get the same deal they could have gotten on their own by working directly with the IRS. These "mills" are a problem all year long, but they tend to be more visible right after the filing season ends and taxpayers are trying to resolve their tax issues perhaps after receiving a balance due notice in the mail.

Suspicious communications

Every form of suspicious communication is designed to trick, surprise, or scare someone into responding before thinking. Criminals use a variety of communications to lure potential victims. The IRS warns taxpayers to be on the lookout for suspicious activity across four common forms of communication: email, social media, telephone, and text messages. Victims are tricked into providing sensitive personal financial information, money, or other information. This information can be used to file false tax returns and tap into financial accounts, among other schemes.

Spear phishing attacks

Spear phishing scams target individuals or groups. Criminals try to steal client data and tax preparers' identities to file fraudulent tax returns for refunds. Spear phishing can be tailored to attack any type of business or organization, so everyone needs to be skeptical of emails requesting financial or personal information.

A recent spear phishing email used the IRS logo and a variety of subject lines such as "Action Required: Your account has now been put on hold" to steal tax professionals' software preparation credentials. The scam email contains a link that if clicked will send users to a website that shows the logos of several popular tax software preparation providers. Clicking on one of these logos will prompt a request for tax preparer account credentials. The IRS warns tax pros not to respond or take any of the steps outlined in the email. The IRS has observed similar spear phishing emails claiming to be from "tax preparation application providers."

The list is not a legal document or a literal listing of agency enforcement priorities. It is designed to raise awareness among a variety of audiences that may not always be aware of developments involving tax administration.

Visit IRS.gov for more information.

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

U.S. Court of Appeals ruling affirms IRS position that abusive microcaptive insurance transactions are shams

IR-2022-118, June 7, 2022

WASHINGTON — The Internal Revenue Service today said that a recent court decision upholds its long-standing position regarding abusive microcaptive insurance transactions. Taxpayers should be alert to these schemes, normally peddled by promoters, as they will ultimately cost them.

On May 12, 2022, in Reserve Mechanical Corp. v. Commissioner, the United States Court of Appeals for the Tenth Circuit appropriately upheld the Internal Revenue Service's position on abusive microcaptive insurance transactions. The Tenth Circuit affirmed the Tax Court's decision holding that the taxpayer was not engaged in the insurance business and that the purported insurance premiums it received were therefore taxable. After the Tax Court decided in favor of the IRS in numerous cases involving microcaptives, Reserve Mechanical is the first appellate decision recognizing the IRS' position that these abusive transactions are shams.

The IRS encourages anyone considering entering a promoted microcaptive insurance transaction to first speak with a qualified, independent advisor. These transactions will result in serious economic loss to taxpayers, including the loss of deductions, required income inclusion and penalties. Taxpayers should understand that the IRS has asserted in many of these cases that the microcaptive insurance transactions lack economic substance and that when transactions are held to lack economic substance, then a 20% penalty (40% if undisclosed) will automatically apply, and it cannot be waived or reduced by the IRS or the courts.

Likewise, taxpayers who have already engaged in such a transaction should speak with a qualified independent tax advisor about their options. The IRS previously offered settlement opportunities for abusive microcaptive transactions, and for taxpayers who come forward seeking to resolve their case, the IRS will consider providing a resolution opportunity as appropriate.

The IRS and Department of Justice will use all available legal options to challenge improper attempts to avoid or evade U.S. income tax, regardless of how long it takes for these cases to wind their way through the courts. The IRS will also aggressively pursue penalties for all participants in these abusive transactions.

-30-

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

IRS-CI releases FY2022 annual report highlighting more than 2,550 investigations, 90% conviction rate; enforcement actions focused on tax fraud, money laundering, cybercrimes

IR-2022-194, Nov. 3, 2022

WASHINGTON — In fiscal year 2022, IRS Criminal Investigation initiated more than 2,550 criminal investigations, identified over $31 billion from tax and financial crimes, and obtained a 90.6% conviction rate on cases accepted for prosecution. The IRS-CI FY22 Annual Report, released Thursday, details these statistics, as well as important partnerships and significant criminal enforcement actions from the past fiscal year, which began Oct. 1, 2021, and ended Sept. 30, 2022.

“The cases the IRS-CI team investigated over the past fiscal year touch multiple continents and require cooperation with partners around the globe. This is why IRS-CI continues to cement itself as the preeminent law enforcement agency investigating financial crimes on a global scale,” said IRS Commissioner Chuck Rettig.

In FY22, IRS-CI expanded partnerships with foreign counterparts to help combat tax and financial crimes on a global level. IRS-CI special agents delivered trainings in countries like Argentina, Germany, Colombia, and Palau on topics ranging from cybercrime to human trafficking. IRS-CI Mexico City, after changes to Mexico law that enabled the extradition of tax fugitives, launched an initiative to identify fugitives who had absconded to Mexico and nearby countries. This initiative resulted in the location of 79 criminal fugitives and the apprehension of eight during the first year.

IRS-CI joined Taskforce Kleptocapture in March 2022 to target Russian oligarchs and other sanctions-evaders. It also worked with the Chiefs of Global Tax Enforcement (J5) to identify potential sanction evaders or sanctioned assets as part of a global strategy to deter Russia’s aggression. As of September 2022, the agency had identified nearly 50 individuals and entities for potential sanctions-related enforcement.

IRS-CI’s 2,077 special agents spent about 70% of their time investigating tax-related crimes like tax evasion and tax fraud during FY22, while nearly 30% of their time was spent on money laundering and drug trafficking cases. Special agents identified over $31 billion from tax and financial crimes, and the agency seized assets valued at approximately $7 billion in FY22. IRS-CI is the only U.S. federal law enforcement agency that focuses 100% on financial investigations.

“Our team follows the money,” said IRS-CI Chief Jim Lee. “We’ve been doing it for more than 100 years, and we’ve followed criminals into the dark web and now into the metaverse. Tax and other financial crimes know no borders. If you violate the law and end up in the crosshairs of an IRS-CI special agent, you are likely going to jail.”

Case examples include:

The IRS-CI Cyber Crime Unit, with assistance from U.S. authorities, traced billions of dollars of Bitcoin stolen from Bitfinex, a cryptocurrency exchange, after a 2016 hack. This led to the February 2022 arrest of Ilya Lichtenstein and his wife, Heather Morgan, for alleged conspiracy to launder stolen cryptocurrency. IRS-CI special agents lawfully seized and recovered more than 94,000 stolen Bitcoin, which was valued at over $3.6 billion at the time, marking the largest seizure in U.S. history.

The Tampa Field Office investigated Michael Dexter Little for tax-related crimes. He was sentenced to 19 years and six months in federal prison in January 2022 for conspiracy to commit wire fraud, conspiracy to commit money laundering and aggravated identity theft. Little also had to forfeit at least $12.3 million,

traceable to his offenses. He filed a series of false tax returns, claiming massive, bogus fuel tax credits. He filed the false returns in his own name and the names of co-conspirators, as well as identity theft victims. He obtained at least $12.3 million in fraudulent tax refunds and attempted to obtain at least $27 million more. Little and his co-conspirators used scheme proceeds to purchase real estate and other assets for themselves.

The Oakland Field Office investigated Jeff and Paulette Carpoff for running a billion-dollar fraud scheme centered around DC Solar. Investors were duped into investing in DC Solar based on fake financial and engineering reports, and the money was used to fund the Carpoffs' lavish lifestyle, which included a NASCAR sponsorship, ownership of a minor league baseball team, luxury real estate and more. The federal government seized and auctioned off 148 of the Carpoffs' vehicles to recoup more than $8 million for scheme victims. In November 2021, Jeff Carpoff was sentenced to 30 years in prison, and in June, Paulette Carpoff was sentenced to 11 years in prison.

The report also includes additional case examples for each U.S. field office, an overview of IRS-CI's international footprint, details about the specialized services provided by IRS-CI and investigative statistics, broken down by discipline, for FY22. Video available for download.

IRS-CI is the criminal investigative arm of the IRS, responsible for conducting financial crime investigations, including tax fraud, narcotics trafficking, money-laundering, public corruption, healthcare fraud, identity theft and more. IRS-CI special agents are the only federal law enforcement agents with investigative jurisdiction over violations of the Internal Revenue Code, boasting a near 90% federal conviction rate. The agency has 20 field offices located across the U.S. and 12 attaché posts abroad.

-30-

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Taxpayer Experience Office formally established to improve service across the IRS

IR-2022-50, March 4, 2022

WASHINGTON – As part of a longer-term effort to improve taxpayer service, the IRS has officially established the first-ever Taxpayer Experience Office and will soon begin taking additional steps to expand the effort.

“As the IRS continues taking immediate steps this filing season including adding more employees to address the significant challenges facing a resource-constrained IRS, it’s critical that we work going forward to equip the IRS to be a 21st century resource for Americans,” said IRS Commissioner Chuck Rettig. “The formal establishment of this office will help unify and expand efforts across the IRS to improve service to taxpayers.”

The Taxpayer Experience Office will focus on all aspects of taxpayer transactions with the IRS across the service, compliance and other program areas, working in conjunction with all IRS business units and coordinating closely with the Taxpayer Advocate Service. The office is part of the effort envisioned in the Taxpayer First Act Report to Congress last year. This included input and feedback from taxpayers, tax professionals and the tax community that helped develop the Taxpayer Experience Strategy. The Report to Congress identified over a hundred different programs and tools that would help taxpayers, including a 360-degree view of taxpayer accounts, expanded e-File and payment options, digital signatures, secure two-way messaging and online accounts for businesses and tax professionals.

To help drive the IRS strategic direction for improving the taxpayer experience, the Taxpayer Experience Office has identified key activities the IRS is focusing on over the next five years, including those commitments outlined in the President’s Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government.

“The IRS is committed to customer experiences that meet taxpayers where they are, in the moments that matter most in people’s lives and in a way that delivers the service that the public expects and deserves,” said Chief Taxpayer Experience Officer Ken Corbin, who also serves as the commissioner of the Wage and Investment division, which oversees the current filing season and other activities.

The Taxpayer Experience Office will identify changing taxpayer expectations and industry trends, focus on customer service best practices, and promote a consistent voice and experience across all taxpayer segments by developing agency-wide taxpayer experience guidelines and expectations. The office will be adding staff in the coming months to help support the effort.

“Whether checking the status of a tax return, meeting with a revenue agent for an audit, or receiving a tax credit to their bank account, improving service delivery and customer experience are fundamental priorities for us,” Corbin said. “We’re committed to designing and delivering services that better connect with our diverse taxpayer base.”

Some of the areas of improvement in the near-term include expanding customer callback, expanded payment options, secure two-way messaging and more services for multilingual customers. These activities build on recent improvements such as digital tools to support Economic Impact Payments and the Advance Child Tax Credit, online chat and online tax professional account.

-30-

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

New IRS Strategic Plan: Agency issues five-year plan with goal to help taxpayers

IR-2022-142, July 20, 2022

WASHINGTON — The Internal Revenue Service today released a new five-year Strategic Plan that outlines its goals to improve taxpayer service and tax administration.

The IRS Strategic Plan FY2022-2026 will serve as a roadmap to help guide the agency's programs and operations. The plan will also help meet the changing needs of taxpayers and members of the tax community.

"Through the Strategic Plan, we want to share our priorities and how they shape the important work that takes place at the IRS, year in and year out, to help taxpayers," said IRS Commissioner Chuck Rettig. "We serve and interact with more Americans than nearly any other public or private organization. The IRS has undergone tremendous change over the last five years, and we continue to evolve to better serve the nation's taxpayers."

The Strategic Plan, developed with input from external partners as well as IRS employees, focuses on four goals that will help improve customer service:

- Service – Provide quality and accessible services to enhance the taxpayer experience.
- Enforcement – Enforce the tax law fairly and efficiently to increase voluntary compliance and narrow the tax gap.
- People – Foster an inclusive, diverse and well-equipped workforce and strengthen relationships with our external partners.
- Transformation – Transform IRS operations to become more resilient, agile and responsive to improve the taxpayer experience and narrow the tax gap.

As the IRS works to achieve these goals, it will continue to uphold taxpayer rights and enforce the tax code fairly to improve the taxpayer experience. Under the Taxpayer Bill of Rights, every taxpayer has fundamental rights of which they should be aware when dealing with the agency.

-30-

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

IRS quickly moves forward with taxpayer service improvements; 4,000 hired to provide more help to people during 2023 tax season on phones

IR-2022-191, Oct. 27, 2022

WASHINGTON – The Internal Revenue Service announced today significant progress to prepare for the 2023 tax filing season as the agency passed a milestone of hiring 4,000 new customer service representatives to help answer phones and provide other services.

These assistors have been hired over the last several months and are being trained to provide help to taxpayers, including answering phone questions. This is part of a much wider IRS improvement effort tied to the Inflation Reduction Act funding approved in August. The IRS continues working hard on implementing the landmark 10-year legislation, and updates on other improvement areas will be provided in the near future.

“The IRS is fully committed to providing the best service possible, and we are moving quickly to use new funding to help taxpayers during the busy tax season,” said IRS Commissioner Chuck Rettig. “Our phone lines have been simply overwhelmed during the pandemic, and we have been unable to provide the help that IRS employees want to give and that the nation’s taxpayers deserve. But help is on the way for taxpayers. As the newly hired employees are trained and move online in 2023, we will have more assistors on the phone than any time in recent history.”

The customer service representatives being hired are in various stages of being onboarded. When they join the IRS, they will receive weeks of training to help serve people and improve the taxpayer experience. The training will cover a wide range of issues including technical account management issues and understanding and respecting taxpayer rights.

The goal is to add another 1,000 customer service representatives by the end of the year, bringing the total of new hires in this area to 5,000.

Many employees will be in place for the start of the 2023 tax season, and others will join as their training is completed in the following weeks. Almost all of their training will be completed by Presidents Day 2023; traditionally the period when the IRS sees the highest phone volumes. The IRS anticipates phones will be answered at a much higher level during the 2023 filing season.

IRS improvements and use of the new direct hire authority have speeded the hiring process. This year, these positions have been brought on since August; last year, it took approximately eight months to hire customer service representatives.

“Even though we have new hires in the pipeline, our phone lines remain extremely busy,” Rettig said. “We continue to urge people to first visit IRS.gov for information related to their tax questions. Many of the questions we receive can be answered online, providing faster answers for people than calling. We appreciate taxpayer’s continued patience with us. Please know that we have dedicated employees across the IRS working hard every day to help people on the phone and in-person. IRS employees look forward to providing better service in the near future.”

In addition to the phone assistors, the IRS is also working to hire additional people throughout the agency, not just in taxpayer service areas but in Information Technology and compliance positions – all with a goal of improving the work the IRS does.

“IRS employees make a difference for our nation, and we’re excited that we can add more people to serve taxpayers and support the critical work of tax administration,” Rettig said. “Positions will be open

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

across the country in coming weeks and months, and we encourage potential candidates to visit USAjobs.gov to look for opportunities."

-30-

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

IRS Appeals revises initial contact letters as part of effort to enhance the taxpayer experience

IR-2022-170, Oct. 4, 2022

WASHINGTON – The Internal Revenue Service Independent Office of Appeals is taking important steps to improve how taxpayers interact and communicate with the IRS by revising their initial contact letters.

“Appeals resolves federal tax disputes, without litigation, in a way that is fair and impartial to taxpayers and the government,” said April Adams-Johnson, the Senior Level Advisor to the Chief of Appeals and Appeals’ first Taxpayer Experience Officer. “Typically, at the start of the process, the Appeals Officer assigned the case sends a letter with some introductory information and invites the taxpayer or their representative to a conference. We want this letter to be clear and easy to understand for all taxpayers.”

Appeals has made two key revisions to these initial contact letters in response to feedback from taxpayers and practitioners.

First, the revised initial contact letter will clarify that generally, taxpayers and representatives can choose how they meet with Appeals through conferences that can be held by telephone, video or in-person. In addition, Appeals can work with taxpayers and representatives through the mail or secure electronic messaging. Appeals employees can successfully resolve disputes in every type of conference and the type of conference does not impact Appeals’ decision.

Second, in addition to the Appeals Officer’s contact information, the initial contact letter will now provide the name and phone number of the Appeals Officer’s manager. While the Appeals Officer remains the primary contact for all their assigned cases, the addition of the manager’s contact information will ensure an appeal stays on track in the rare instance additional help is needed.

Going forward, taxpayers and representatives will see the new language providing manager contact information and clarifying conference choice in the initial contact letters sent for most cases received in Appeals, including cases relating to an IRS examination determination, penalties, an offer in compromise, a request for a Collection Due Process hearing or participation in IRS e-file.

“We recognize that improving the taxpayer experience is a continuing process,” said Adams-Johnson. “Appeals welcomes comments on additional ways we can help create a more positive experience for taxpayers and representatives, whether through revisions to our communications or through other process improvements.”

Individuals may submit their comments to AP.Taxpayer.Experience@irs.gov by Dec. 2, 2022.

-30-

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

IRS Independent Office of Appeals' priorities for 2023 focus on taxpayer service

IR-2022-195, Nov. 4, 2022

WASHINGTON – Today, the IRS Independent Office of Appeals released its focus guide for fiscal year 2023. Appeals is taking important steps to expand communications with external stakeholders and to improve taxpayer access to Appeals. Promoting transparency and taxpayer access helps Appeals fulfill its mission to resolve tax disputes in a fair and impartial manner without the need for litigation.

The focus guide outlines the taxpayer service initiatives you can expect over the coming year, including:

- Increasing stakeholder outreach – including to historically marginalized and limited English proficient communities – about the appeals process
- Improving access to in-person and video conferences and revising letters and notices to ensure taxpayers understand that it is generally their choice how to meet with Appeals
- Leveraging technology to improve how Appeals works and manages its cases
- Continuing the *Practitioner Perspectives* series in which tax practitioners share insights and feedback with Appeals employees. Recordings of prior panel discussions on Collection Appeals and Examination Appeals are available
- Developing training for Appeals employees on enhancing customer engagement

"We are excited to share Appeals' 2023 priorities," said Andy Keyso, Chief of Appeals. "We will keep doing all we can to promote a positive experience for taxpayers and practitioners, while building upon our past accomplishments and applying lessons we learned from the challenges posed by COVID-19."

A key success in 2022 is how Appeals addressed a significant increase in cases referred for settlement after the taxpayer filed a petition in the United States Tax Court. Many of these cases involved taxpayers without legal representation and resulted from communications challenges and difficulties in obtaining and sharing documents during the pandemic.

To avoid further delays, Appeals prioritized these docketed cases and dedicated additional resources to promptly resolve them. Appeals shared guidelines for how employees would streamline their approach to these cases with the public in April 2022. Under these guidelines, Appeals attempted to reach affected taxpayers by telephone shortly after receiving the cases. In addition, Appeals considered specific-dollar settlements, expedited tax computation, and streamlined internal documentation of proposed settlements. As always, Appeals Officers applied their professional judgment, including to accept oral testimony where appropriate, to settle the cases efficiently.

Using this approach, Appeals resolved all 7,500 docketed cases pending when the initiative began. To achieve permanent improvements to the taxpayer experience, the IRS is working to increase the number of cases resolved at the earliest stage possible—before a dispute arises.

"Ensuring that taxpayers and practitioners are satisfied with the appeals process is an ongoing goal for us," said Shahid Babar, Acting Deputy Chief of Appeals. "The 2023 focus guide is a way to share with the public and with employees our ideas for continually improving how Appeals resolves tax disputes."

-30-

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

2023 PTIN renewal period underway for tax professionals

IR-2022-190, Oct. 27, 2021

WASHINGTON — The Internal Revenue Service urges the nation's more than 750,000 active tax return preparers to start the upcoming 2023 filing season smoothly by renewing their Preparer Tax Identification Numbers (PTINs) now. All current PTINs will expire Dec. 31, 2022.

Anyone who prepares or helps prepare a federal tax return for compensation must have a valid PTIN from the IRS before preparing returns, and they need to include the PTIN as the identifying number on any return filed with the IRS.

The fee to renew or obtain a PTIN is $30.75 for 2023. The PTIN fee is non-refundable.

Tax return preparers with a 2022 PTIN should use the online renewal process, which takes about 15 minutes to complete. A paper option, Form W-12, along with the instructions, is also available for PTIN applications and renewals. However, the paper form can take four to six weeks to process. Failure to have and use a valid PTIN may result in penalties.

To renew a PTIN online:

- Start at IRS.gov/taxpros.
- Select the “Renew or Register” button.
- Select “Log in” and enter the user ID and password to access the online PTIN system.
- Select the “Renew my PTIN” button from the main menu.

Once completed, users will receive confirmation of their PTIN renewal.

The online system not only allows PTIN renewal but tax return preparers may receive communications through a secure mailbox from the IRS Return Preparer Office.

First-time PTIN applicants can also apply for a PTIN online.

To apply for a PTIN online:

- Start at IRS.gov/taxpros.
- Select the “Renew or Register” button.
- Select "Create an Account" and follow the prompts to complete the account setup process and obtain a temporary password.
- Log in and follow the remaining steps to access the online PTIN system.
- Select the “Register for a PTIN” button from the main menu.

PTIN system enhancements

The online PTIN system has a new look and feel for a more optimized preparer experience when renewing or registering for a PTIN. Improvements include:

- **Dynamic application design** – system dynamically adapts based on the preparer’s responses and guides them to the correct application.
- **Mobile responsive/mobile friendly** – system will adjust to device’s screen size.

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

- **Multi-year renewals/registrations** – preparers can renew/register for multiple calendar years at one time.
- **Expanded Support Channel** – webchat available for assistance with PTIN account questions.

Opportunity for non-credentialed tax preparers

The Annual Filing Season Program is a voluntary IRS program intended to encourage non-credentialed tax return preparers to take continuing education courses to increase their knowledge and improve their filing season readiness.

Those who choose to participate must renew their PTIN, complete up to 18 hours of continuing education from IRS-approved CE providers and consent to adhere to specific obligations in Circular 230 by Dec. 31, 2022.

After completing the steps, the return preparer receives an Annual Filing Season Program Record of Completion from the IRS. Program participants are then included in a public directory of return preparers with credentials and select qualifications on the IRS website.

The searchable IRS directory helps taxpayers find preparers in their area who have completed the program or hold professional credentials recognized by the IRS.

Enrolled agent credential

The enrolled agent credential is an elite certification issued by the IRS to tax professionals who demonstrate special competence in federal tax planning, individual and business tax return preparation and representation matters. Enrolled agents have unlimited representation rights, allowing them to represent any client before the IRS on any tax matter.

As non-credentialed return preparers think about next steps in their professional career, the IRS encourages them to consider becoming an enrolled agent.

All enrolled agents, regardless of whether they prepare returns, must renew their PTIN annually to maintain their active status.

-30-

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

IRS updates tax gap estimates; new data points the way toward enhancing taxpayer service, compliance efforts

IR-2022-192, October 28, 2022

WASHINGTON — The Internal Revenue Service today released a new set of tax gap estimates on tax years 2014 through 2016 showing the estimated gross tax gap increased to $496 billion, a rise of over $58 billion from the prior estimate.

The gross tax gap is the difference between estimated 'true' tax liability for a given period and the amount of tax that is paid on time. As discussed below, it is important to note that the tax gap estimates cannot fully account for all types of evasion.

"These findings underscore the importance of ensuring fairness in our nation's tax system," said IRS Commissioner Chuck Rettig. "The increase in the tax gap estimates reflects that the IRS needs to do more, both in improving taxpayer service as well as working to improve tax compliance. The IRS remains committed to ensuring fairness and helping taxpayers while also working to better identify emerging compliance issues that contribute to the tax gap. The recent funding addition will help the IRS in many ways, increasing taxpayer education, significantly improving service to all taxpayers and focusing on high-income/high-wealth non-compliance in a fair and impartial manner supporting compliant taxpayers."

After late payments and IRS efforts collected an additional $68 billion, the IRS estimated the net tax gap was $428 billion. This increase in the tax gap can be attributed to economic growth.

Between the two periods, 2011-2013 and 2014-2016, the estimated tax liability increased by more than 23 percent.

The tax gap estimates translate to about 85% of taxes paid voluntarily and on time, which is in line with recent levels. The new estimate is a slight improvement from 83.7 percent in a revised Tax Year 2011-2013 estimate, which dipped slightly from the original estimate released earlier. After IRS compliance efforts are taken into account, the estimated share of taxes eventually paid is 87% for 2014-2016.

The gross tax gap comprises three components:

- Nonfiling (tax not paid on time by those who do not file on time, $39 billion),
- Underreporting (tax understated on timely filed returns, $398 billion), and
- Underpayment (tax that was reported on time, but not paid on time, $59 billion).

A particular challenge for tax gap estimation is the time it takes to collect compliance data, especially data on underreporting that come from completed examinations (audits). To address this issue, the current release includes estimated tax gap projections for Tax Years 2017-2019.

Based on the projections for 2017-2019, the estimated average gross tax gap is projected to be $540 billion per year. The associated voluntary compliance rate is projected to be 85.1 percent. The projection of enforced and other late payments is $70 billion, which yields a net tax gap projection of $470 billion. The associated non-compliance rate projection is 87.0 percent.

The gross tax gap nonfiling, underreporting, and underpayment component projections for Tax Years 2017-2019 timeframe are $41 billion, $433 billion, and $66 billion respectively.

As part of the larger effort to reduce the actual tax gap, the IRS will continue to fairly enforce the tax laws. In 2021, the latest year for which data is available, the IRS currently collected more than $4 trillion in taxes, penalties, interest and user fees.

Tax gap studies through the years have consistently demonstrated that third-party reporting of income significantly raises voluntary compliance with the tax laws. And voluntary compliance rises even higher when income payments are also subject to withholding. The IRS also has an array of other taxpayer service programs aimed at supporting accurate tax filing and helping address the tax gap. These range

from working with businesses and partner groups to a variety of education and outreach efforts.

The voluntary compliance rate of the U.S. tax system is vitally important for the nation. A one-percentage-point increase in voluntary compliance would bring in about $40 billion in additional tax receipts.

The tax gap estimates provide insight into the historical scale of tax compliance and to the persisting sources of low compliance.

"Keeping the voluntary compliance rate as high as possible ensures that taxpayers believe our system is fair," Rettig said. "The vast majority of taxpayers strive to pay what they owe on time. Those who do not pay their fair share ultimately shift the tax burden to those people who do, which fuels the tax gap. The IRS will continue to direct our resources to help educate taxpayers about the tax requirements under the law while also focusing on pursuing those who avoid their legal responsibilities."

Estimating the tax gap; offshore, digital assets, other categories not fully represented

Given the complexity of the tax system and available data, no single approach can be used for estimating each component of the tax gap. Each approach is subject to measurement or nonsampling error; the component estimates that are based on samples are also subject to sampling error. For the individual income tax underreporting tax gap, Detection Controlled Estimation is used to adjust for measurement errors that results when some existing noncompliance is not detected during an audit. Other statistical techniques are used to control for bias in estimates based on operational audit data. Because multiple methods are used to estimate different subcomponents of the tax gap, no standard errors are reported. In addition, those reviewing this data should be mindful of these limitations when using these estimates.

Given available data, these are the best possible estimates of the tax gap components presented, although they do not represent the full extent of potential non-compliance. There are several factors to keep in mind:

- The estimates cannot fully represent noncompliance in some components of the tax system including offshore activities, issues involving digital assets and cryptocurrency as well as corporate income tax, income from flow-through entities, illegal activities because data are lacking.
- The tax gap associated with illegal activities has been outside the scope of tax gap estimation because the objective of government is to eliminate those activities, which would eliminate any associated tax.
- For noncompliance associated with digital assets and other emerging issues, it takes time to develop the expertise to uncover associated noncompliance and for examinations to be completed that can be used to measure the extent of that noncompliance.

The IRS continues to actively work on new methods for estimating and projecting the tax gap to better reflect changes in taxpayer behavior as they emerge.

Additional information:

- Federal Tax Compliance Research: Tax Gap Estimates for Tax Years 2014–2016 (Publication 1415) **PDF**
- Tax Gap Executive Summary (Publication 5364) **PDF**
- Tax Gap Map (Publication 5365) **PDF**

— 30 —

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

IRS Advisory Council issues 2022 Annual Report

IR-2022-200, Nov. 16, 2022

WASHINGTON — The Internal Revenue Service Advisory Council (IRSAC) today issued its annual report for 2022, including recommendations to the IRS on new and continuing issues in tax administration.

The 2022 Public Report includes recommendations on 21 issues covering a broad range of topics including:

- IRS business and information technology modernization.
- Reduction in electronic filing threshold for information return filers.
- Alignment of electronic signature requirements on withholding certificates.
- Accelerated issuance of IRS Form 6166, Certification of U.S. Residency.
- The Examination Customer Coordination and Innovation Office.
- Series 8038 Form Redesign and Updates.
- Business Master File (BMF) Transcript Delivery Service (TDS).

In addition, the report "emphasizes the need for consistent and multi-year funding for the IRS to achieve its goals of providing efficient, effective, modern service to the nation's taxpayers." It also "provides targeted feedback to improve the taxpayer experience while supporting crucial enforcement efforts and navigating a rapidly changing digital environment."

The IRSAC serves as a federal advisory committee to the IRS commissioner that provides an organized public forum for discussion of relevant tax administration issues between IRS officials and representatives of the public. IRSAC members offer constructive observations regarding current or proposed IRS policies, programs and procedures.

The IRSAC is administered under the Federal Advisory Committee Act by the Office of National Public Liaison, part of IRS Communications and Liaison, and draws its members from the taxpaying public, the tax professional community, representatives of the low-income community, small and large businesses, tax-exempt and government entities, the payroll industry and academia. Five subgroups report to the parent council:

- Information Reporting
- Large Business & International
- Small Business/Self-Employed
- Tax Exempt/Government Entities
- Wage & Investment

Acting Commissioner Doug O'Donnell and IRS executives thanked 10 members of the council whose terms end this year:

- **W. Edward Afield** – Afield served on the Small Business/Self Employed Subgroup.
- **Robert Howren** – Howren served on the Large Business & International Subgroup.
- **Denise Jackson** – Jackson served on the Wage & Investment Subgroup.
- **Kathleen Lach** – Lach served on the Small Business/Self Employed Subgroup.
- **Carol Lew** – Lew served as Chair of IRSAC.
- **Kelly Myers** – Myers served on the Small Business/Self Employed Subgroup.
- **Joseph Novak** – Novak served as Chair of the Large Business & International Subgroup.

- **Robert Panoff** – Panoff served as Chair of the Small Business/Self Employed Subgroup.
- **Katie Sunderland** – Sunderland served on the Large Business & International Subgroup.
- **Kevin Valuet** – Valuet served on the Information Reporting Subgroup.

The full 2022 IRSAC Public Report is available at IRS.gov.

-30-

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Online seminars from 2022 IRS Nationwide Tax Forum now available

IR-2022-176, Oct. 11, 2022

WASHINGTON –Those who may have missed the 2022 IRS Nationwide Tax Forum now have a second chance to view the seminars and earn continuing education credit through the 2022 Nationwide Tax Forums Online.

The online version of the forum consists of 18 new self-study seminars that use interactive videos, PowerPoint slides and transcripts to educate tax professionals. This year, the online version includes four Spanish-language seminars.

The 2022 Nationwide Tax Forums Online includes the following seminars:

- IRS Commissioner Chuck Rettig's Keynote Address
- Tax Law Changes for Tax Year 2022 -- in English and Spanish
- Professional Responsibility Obligations (ethics) – in English and Spanish
- Tax Treatment of Digital Assets
- Tax-Exempt Organizations Update
- Emerging Cyber Crimes – in English and Spanish

The Nationwide Tax Forums Online is registered as a qualified sponsor of continuing education with the IRS Return Preparer Office and the National Association of State Boards of Accountancy. For a fee, CPAs, Enrolled Agents and Annual Filing Season Program participants can earn continuing education credit.

The online forum seminars can also be reviewed for free. Individuals who choose to review (or audit) the seminars will not receive continuing education credit.

In addition to the newly added 2022 seminars, numerous seminars from prior IRS Tax Forums are also available.

For more information and to access the seminars, visit www.irstaxforumsonline.com.

-30-

Check here for prior posts and new updates.

www.irs.gov/a-closer-look

A CLOSER LOOK

"A Closer Look" is a new area on the IRS website that will cover a variety of timely issues of interest to taxpayers and the tax community. It will also provide a detailed look at key issues affecting everything from IRS operations and employees to issues involving taxpayers and tax professionals.

Take a closer look.

Follow IRS

Verify accounts at **IRS.gov/socialmedia**

Publication 5468 (11-2020) Catalog Number 75115W Department of the Treasury **Internal Revenue Service** www.irs.gov