# Publication 1345

# Authorized IRS e-file Providers of Individual Income Tax Returns

## Volume 1 of 2


***Get forms and other information faster and easier at:***

- ***IRS.gov*** (English)
- ***IRS.gov/Spanish*** (Español)
- ***IRS.gov/Chinese*** (中文)
- ***IRS.gov/Korean*** (한국어)
- ***IRS.gov/Russian*** (Русский)
- ***IRS.gov/Vietnamese*** (Tiếng Việt)

Publication 1345 (Rev. 11-2023) Catalog Number 39371M
Department of the Treasury **Internal Revenue Service** www.irs.gov

Visit the Accessibility Page on IRS.gov

This page is intentionally left blank

# Table of Contents

# Chapter 1 – Stay Informed

## What's New in Publication 1345?

This edition of Publication 1345, Handbook for Authorized IRS *e-file* Providers of Individual Income Tax Returns replaces the previous edition revised November 2022.

- Added Publication 5708, Creating a Written Information Security Plan for Your Tax & Accounting Practice to Publications for Individual Income Tax Returns
- Added multi-factor authentication to the basic security steps in Safeguarding IRS *e-file*
- Added a paragraph to Safeguarding IRS *e-file* stating providers must require taxpayers who have established an online account to validate access to a second factor (email, phone or other secure

authenticator) before being permitted to electronically transmit their tax return to the IRS

- Added a statement to Safeguarding IRS *e-file* from Fraud and Abuse regarding returns related to identity theft refund fraud
- Updated form descriptions in Submission of Paper Documents to the IRS
- Added definition for “Multi-factor” to the Glossary
- Grammatical and editorial changes made and links updated throughout the publication

## Where to Get Additional Information?

The IRS offers Providers several sources of information for frequently asked questions.

**Where can I find the most current information about IRS e-file?**

Visit "**Tax Pros.**"

**How does the IRS keep Authorized IRS e-file Providers (Providers) informed of operational developments and issues?**

The IRS posts all important operations information at IRS.gov.

The IRS also notifies Providers of important information via "QuickAlerts" e-file Messaging System and various other subscription services.

- **QuickAlerts** – Provides a free Online messaging system that sends emails to all subscribers, keeping Tax Professionals updated on all e-file related issues and events.
- **IRS Newswire** – Provides news releases and other documents via e-mail as the IRS National Media

Relations Office in Washington, DC issues them.

- **IRS Tax Tips** – Provides tax information via e-mail from the IRS daily during the tax-filing season and periodically the rest of the year.
- **Tax Stats Dispatch Mailing List** – Provides announcements via e-mail which cover the most recent tax statistics.
- **e-News for Small Businesses** – Provides information about IRS Small Business and Self-Employed (SB/SE) outreach products and programs via e-mail.
- **IRS GuideWire** – Provides advance copies of tax guidance such as Revenue Rulings, Revenue Procedures, Announcements and Notices by e-mail.

- **e-News for Tax Professionals** – Provides the latest IRS updates for the tax professional community.

**Where can I find the current filing season information I need?**

The IRS updates **Modernized e-file (MeF) program** information prior to each filing season.

**If I get correspondence from the IRS, who can I call for more information?**

All letters from the IRS have a contact telephone number to reach the person best able to help you with your questions.

**Where can I find telephone numbers and addresses for other services provided by the IRS?**

Providers may find addresses and telephone numbers for their clients at **Let Us Help You.**

**What information should I give taxpayers so they can inquire about the**

**status of their individual income tax refunds?**

Taxpayers and Tax Professionals should be advised to check the status of their individual income tax refunds using **Where's My Refund?**

**Where can I or my customers get information about electronic payment options?**

Taxpayers and Tax Professionals can find information about electronic payment options at **Pay Online.**

**How Do I Report Suspected Tax Fraud Activity?**

If you suspect or know of an individual or company that isn't complying with the tax laws, see "**How Do You Report Suspected Tax Fraud Activity?**"

**What if my software doesn't work, what should I do?**

The IRS does not develop or sell tax preparation or electronic return data transmission software. If problems exist, Providers should contact the vendor who sold them the software or the technical support operation that comes with the software package.

**Where can I get information about the IRS Nationwide Tax Forums?**

This information can be found at **IRS Nationwide Tax Forum Information**.

**Where can I get more information about filing both federal and state individual income tax returns?**

Additional information is available at **TIGERS MODERNIZED EFILE (MeF)** – **FED/STATE EFILE PROGRAMS**. Often, the Provider offering comprehensive one-stop tax service is the most successful. If the Provider isn't participating in Federal/State e-file, it is missing a business opportunity to offer its

clients and customers the benefits and convenience of filing both federal and state tax returns electronically.

# Chapter 2 – Must Read

## Publications for Individual Income Tax Returns

This publication, Publication 1345, Handbook for Authorized IRS *e-file* Providers of Individual Income Tax Returns, provides rules and requirements for participation in IRS *e-file* of individual income tax returns and related forms and schedules. Violating a provision of this publication may subject the Authorized IRS *e-file* Provider (Provider) to sanctions. Providers should familiarize themselves with **Revenue Procedure 2007-40**, 2007-26 I.R.B. 1488 (or the latest update) and **Publication 3112, IRS *e-file* Application and Participation**, to ensure compliance with requirements for participation in IRS *e-file*. The IRS revises Publication 1345 annually.

**Publication 4164, Modernized *e-file* (MeF) Guide for Software Developers and**

**Transmitters**. This publication outlines the communication procedures, transmission formats, business rules and validation procedures for returns e-filed through the Modernized e-file (MeF) system.

**Publication 4557, Safeguarding Taxpayer Data, A Guide for Your Business**. This publication provides helpful information on safeguarding taxpayer data including how to create a data security plan.

**Publication 5708, Creating a Written Information Security Plan for Your Tax & Accounting Practice.** Publication 5708 will be used by Tax and Accounting practices for information on developing an Information Security Plan. The publication was developed during the Security Summit, jointly by private sector companies, State and local tax agencies and the IRS.

# Safeguarding IRS *e-file*

Safeguarding of IRS *e-file* from fraud and abuse is the shared responsibility of the IRS and Authorized IRS *e-file* Providers. Providers must be diligent in recognizing and preventing fraud and abuse in IRS *e-file*. Neither the IRS nor Providers benefit when fraud or allegations of abuse tarnish the integrity and reputation of IRS *e-file*. Providers must report fraud and abuse to the IRS as indicated in the "**Where to Get Additional Information?**" section. Providers must also cooperate with IRS investigations by making available to the IRS, upon request, information and documents related to returns with potential fraud or abuse.

Safeguarding taxpayer data is a top priority for the IRS. It is the legal responsibility of government, businesses, organizations, and individuals that receive, maintain, process, share, transmit or store taxpayers' personal information. Taxpayer data is defined as any

information that is obtained or used in the preparation of a tax return (e.g., income statements, notes taken in a meeting, or recorded conversations). Putting safeguards in place to protect taxpayer information helps prevent fraud and identity theft and enhances customer confidence and trust.

Protecting taxpayer data is required by law. Federal law gives the Federal Trade Commission (FTC) authority to set data safeguard regulations for various entities, including professional tax return preparers. According to the FTC Safeguards Rule in Part 314 (16 C.F.R.), tax return preparers must create and enact security plans to protect client data. Failure to do so may result in a FTC investigation.

The FTC also works to protect taxpayer data. Providers subject to the Gramm-Leach-Bliley Act must follow the FTC's Financial Privacy and Safeguard Rules. The Safeguards Rule requires the protection of the security,

confidentiality and integrity of customer information by implementing and maintaining a comprehensive information security program. The program must include administrative, technical, and physical safeguards appropriate to the business's size, the nature and scope of its activities, and the sensitivity of the customer information at issue.

Here are a few basic security steps:

- Recognize phishing emails
- Create a data security plan
- Review internal controls
- Report any data theft or loss
- Implement multi-factor authentication for anyone accessing taxpayer information. This is required under FTC Safeguards Rule Part 314, (16 C.F.R).

All persons and entities who receive taxpayers' personal information can use

**Publication 4557, Safeguarding Taxpayer Data, A Guide for Your Business**, to help determine their data privacy and security needs and implement safeguards to protect the information. Publication 4557 includes information about security standards and best practice guidelines to safeguard consumer information such as personal tax data, with links to several resources including National Institute of Standards and Technology (NIST) publications. Not taking necessary steps to implement or correct your security program may result in sanctions from the FTC. Failures that lead to an unauthorized disclosure may subject you to penalties under sections 7216 and/ or 6713 of the Internal Revenue Code (I.R.C.).

At a minimum, providers must require taxpayer's who have established an online account to validate access to a second factor (email, phone or other secure authenticator) before being permitted to electronically

transmit their tax return to the IRS. For a taxpayer creating a new account, this requires validation of the phone number, email, or other secure authenticator prior to electronically submitting a tax return. For a taxpayer logging back into an existing account, this requires multi-factor authentication of the taxpayer prior to granting access to tax data stored within the account. Multi-factor authentication requires the use of at least two of the these authentication factors: a knowledge factor (for example, a password); a possession factor (for example, a token); and an inherence factor (for example, biometric).

Providers appoint an individual as a Responsible Official who is responsible for ensuring the firm meets IRS *e-file* rules and requirements. Providers with problems involving fraud and abuse may be suspended or expelled from participation in IRS *e-file*, be

assessed preparer and other civil penalties or be subject to legal action.

## IRS *e-file* Security, Privacy and Business Standards

The IRS has mandated six security, privacy, and business standards to supplement the Gramm-Leach-Bliley Act to better serve taxpayers and protect their information collected, processed and stored by Online Providers of individual income tax returns. The first five standards continue to apply to Online Providers, while Standard number six, "Reporting of Security Incidents," is now mandated for all Providers.

Individual income tax returns refer to the 1040 family of returns. Refer to the **IRS Publication 3112, IRS e-file Application and Participation**, for definition of Online Provider.

The security and privacy objectives of these standards are:

- Setting minimum encryption standards for transmission of taxpayer information over the internet and authentication of website owner/operator's identity beyond that offered by standard version SSL certificates.
- Periodic external vulnerability scan of the taxpayer data environment.
- Protection against bulk-filing of fraudulent income tax returns.
- The ability to timely isolate and investigate potentially compromised taxpayer information.

These standards also address certain business and customer service objectives, such as instant payment options, access to website owner/operator's contact information, and Online Provider's written commitment to maintaining physical, electronic, and procedural safeguards of taxpayer information

that comply with applicable law and federal standards.

- Extended Validation SSL Certificate

  Online Providers of individual income tax returns must have a valid and current Extended Validation Secure Socket Layer (SSL) certificate using TLS 1.2 or later and minimum 2048-bit RSA/128-bit AES.

- External Vulnerability Scan

  Online Providers of individual income tax returns must contract with an independent third-party vendor to run weekly external network vulnerability scans of all their "system components" in accordance with the applicable requirements of the **Payment Card Industry Data Security Standards (PCIDSS).** All scans must be performed by a scanning vendor certified by the **Payment Card**

**Industry Security Standards Council** and listed on their current list of **Approved Scanning Vendors (ASV)**. In addition, Online Providers of individual income tax returns whose systems are hosted must ensure that their host complies with all applicable requirements of the **PCIDSS**.

For the purposes of this standard, "system components" is defined as any network component, server, or application that is included in or connected to the taxpayer data environment. The taxpayer data environment is that part of the network that has taxpayer data or sensitive authentication data.

If scan reports reveal vulnerabilities, action must be taken to address the vulnerabilities in line with the scan report's recommendations. Retain weekly scan reports for at least one

year. The ASV and the host (if present) must be in the United States.

- Information Privacy and Safeguard Policies

  This standard applies to Authorized IRS *e-file* Providers participating in Online Filing of individual income tax returns that own or operate a website through which taxpayer information is collected, transmitted, processed or stored. These Providers must have a written information privacy and safeguard policy consistent with the applicable government and industry guidelines and including the following statement: “we maintain physical, electronic and procedural safeguards that comply with applicable law and federal standards.”

  In addition, Providers’ compliance with these policies must be certified by a

**privacy seal vendor** acceptable to the IRS.

- Protection Against Bulk Filing of Fraudulent Income Tax Returns

  This standard applies to Online Providers of individual income tax returns that own or operate a website through which taxpayer information is collected, transmitted, processed or stored. These Online Providers must implement effective technologies to protect their website against bulk filing of fraudulent income tax returns. Taxpayer information must not be collected, transmitted, processed or stored otherwise.

- Public Domain Name Registration

  This standard applies to Online Providers of individual income tax returns that own or operate a website through which taxpayer information is

collected, transmitted, processed or stored. These Online Providers must have their website's domain name registered with a domain name registrar that is in the United States and accredited by the **Internet Corporation for Assigned Names and Numbers (ICANN)**. The domain name must be locked and not be private.

- Reporting of Security Incidents

  Authorized IRS *e-file* Providers of individual income tax returns must report security incidents to the IRS as soon as possible but not later than the next business day after confirmation of the incident. For the purposes of this standard, an event that can result in an unauthorized disclosure, misuse, modification, or destruction of taxpayer information (e.g., breach)

must be considered a reportable security incident.

Providers with multiple roles must follow instructions for submitting incident reports at "**Instructions for Reporting Security Incidents**."

Those that are EROs only must contact their local stakeholder liaison by following the instructions at "**Data Theft Information for Tax Professionals.**"

In addition, if the Provider's website is the cause of the incident, the Provider must cease collecting taxpayer information via their website immediately upon detection of the incident and until the underlying causes of the incident are successfully resolved.

## Returns Filed Using IRS *e-file*

A return filed using IRS *e-file* may be a composite of electronically transmitted data and certain paper documents or be completely paperless. The paper portion of a composite return may consist of **Form 8453, U.S. Individual Income Tax Transmittal for an IRS *e-file* Return**, and other paper documents that cannot be electronically transmitted are attached to the form and mailed to the IRS (See **Submitting the Electronic Return to the IRS**).

Filing individual income tax returns using IRS *e-file* is limited to tax returns with prescribed due dates in the current year and two previous years. A taxpayer can electronically file an individual income tax return year-round except for a short cutover period at the end of the calendar year.

If Providers submit state individual income tax returns as part of Federal/State e-file,

state returns become a part of the electronically transmitted data. States often require the submission of paper documents to complete the return, but they are separate from paper documents for federal returns. Providers should process state paper documents according to applicable state rules.

## Returns Not Eligible for IRS *e-file*

The following individual income tax returns and related return conditions cannot be processed using IRS *e-file*:

- Tax returns with fiscal year tax periods;
- Returns with forms or schedules that can’t be processed by IRS *e-file*;
- Tax returns with Taxpayer Identification Numbers (TIN) within the range of 900-00-0000 through 999-99-9999. Exception: Adoption

Taxpayer Identification Numbers (ATIN) and Individual Taxpayer Identification Numbers (ITIN) may fall within the range above. Valid ATINs have the digits 93 in the fourth and fifth positions. Valid ITINs have digits within a range of 50 through 65, 70 through 88, 90 through 92 and 94 through 99 in the fourth and fifth positions. See **"Verifying Taxpayer Identity and Taxpayer Identification Numbers (TINs)"** for more information on ATINs and TINs; and

- Tax returns that the IRS cannot electronically process because the returns have rare or unusual processing conditions or that exceed the specifications for returns allowable in IRS *e-file*. These conditions change from year to year. The software should alert Providers to these conditions

when they occur. If Providers transmit electronic return data with one of these conditions to the IRS, the transmission rejects, and the taxpayer may have to file the tax return on paper. The software package documentation or the software's support program should provide information that is more specific.

## Submitting a Timely Filed Electronic Tax Return

All prescribed due dates for filing of returns apply to e-file returns. All Providers must ensure that returns are promptly processed. A Provider that receives a return for electronic filing on or before the due date of the return (including extensions) must ensure that it transmits the electronic part of the return on or before the due date. An electronically filed return isn't considered filed until the IRS acknowledges acceptance of the electronic part of the tax return for processing. The IRS

accepts individual income tax returns electronically only if the taxpayer signs the return using a Personal Identification Number (PIN). If Providers transmit the electronic portion of a return on or shortly before the due date and the IRS ultimately rejects it, but the Provider and the taxpayer comply with the requirements for timely resubmission of a correct return, the IRS considers the return timely filed. For additional information about the filing of a return through IRS *e-file*, see "**Submitting the Electronic Return to the IRS**."

Transmitters may provide electronic postmarks to taxpayers for individual returns if the Transmitters follow the requirements stated in "**Chapter 4 – Transmission**." The receipt of an electronic postmark provides taxpayers with confidence that they have filed their return timely. The date of the electronic postmark is considered the date of filing when the date of electronic postmark is on or

before the prescribed due date and the return is received by the IRS after the prescribed due date for filing. All requirements for signing the return and completing a paper declaration, if required, as well as for timely resubmitting of a rejected timely filed return, must be adhered to for the electronic postmark to be considered the date of filing.

## Federal/State *e-file*

Federal/State e-file is a cooperative tax filing effort between the IRS and most states, which allows Providers to file federal and state returns electronically to IRS. The state return can be sent linked to the federal return (by including the Submission ID of the federal return in the state submission), or it can be sent unlinked (standalone). On linked returns, the federal return must be accepted before the linked state return can be filed. In addition to accepting federal and state individual income tax returns electronically in

a single transmission, state-only returns are also accepted if the return:

- was previously rejected by the state;
- is originated separately from the federal return;
- is a part-year residency return;
- is a non-resident state return; or
- is a married filing separately state return, but the federal return was filed jointly.

The IRS provides state acknowledgment services. Participating states can send their acknowledgment to the IRS for Transmitters to pick up when they pick up their federal acknowledgment.

Adding Federal/State e-file to a Provider's business is like the process it went through to become a Provider. Refer to **Publication 3112, IRS *e-file* Application and Participation**, for further details. Also, the

Provider should contact the state coordinators for the state programs in which it participates for further explanation of state rules and requirements.

This page is intentionally left blank

# Chapter 3 – Electronic Return Origination

## Obtaining, Handling and Processing Return Information from Taxpayers

An Electronic Return Originator (ERO) begins the process of electronic submission of returns it either prepares or collects from taxpayers who want to e-file their returns. An ERO starts the electronic submission of a return after the taxpayer authorizes the filing of the return via IRS *e-file*. The ERO must have either prepared the return or collected it from a taxpayer or another authorized ERO. An ERO begins the electronic submission by:

- electronically sending the return to a Transmitter that transmits the return to the IRS;

- directly transmitting the return to the IRS (must also have a Transmitter role); or,
- providing a return to an Intermediate Service Provider for processing prior to transmission to the IRS.

The ERO must always identify the paid tax return preparer (if any) in the proper field of the electronic record of returns. The ERO must enter the paid preparer's identifying information (name, address, Employer Identification Number (EIN), when applicable, and Preparer Tax Identification Number (PTIN). EROs may either transmit returns directly to the IRS or arrange with another Provider to transmit the electronic return to the IRS.

A Provider, including an ERO, may disclose tax return information to other Providers relating to e-filing a tax return under Treas. Reg. §301.7216-2(d)(1) without obtaining the taxpayer's consent. For example, an ERO may

pass on return information to an Intermediate Service Provider or a Transmitter for the purpose of having an electronic return formatted or transmitted to the IRS.

An ERO that chooses to originate returns that it has not prepared, but only collected, becomes a tax return preparer of the returns when, as a result of entering the data, it discovers errors that require substantive changes and then makes the changes. A non-substantive change is a correction limited to a transposition error, misplaced entry, spelling error or arithmetic correction. The IRS considers all other changes substantive, and the ERO becomes a tax return preparer. As such, the ERO must sign the tax return as a tax return preparer.

## Safeguarding IRS *e-file* From Fraud and Abuse

Safeguarding taxpayers and IRS *e-file* from identity theft refund fraud requires that

Providers be diligent in detecting and preventing identity theft fraud patterns and schemes. Early detection of these patterns and schemes is critical to stopping them and their adverse impacts, and to protecting taxpayers and IRS *e-file*. While all Providers must be on the lookout for fraud and abuse in IRS *e-file*, EROs must be particularly diligent while acting in their capacity as the first contact with taxpayers filing a return. An ERO must be diligent in recognizing fraud and abuse, reporting it to the IRS and preventing it when possible. This includes not submitting returns to the IRS when there is a high likelihood the return is related to identity theft refund fraud. Providers must cooperate with IRS investigations by making available to the IRS, upon request, information and documents related to returns with potential fraud or abuse.

Indicators of abusive or fraudulent returns may be unsatisfactory responses to filing

status questions, multiple returns with the same address, and missing or incomplete Schedules A and C income and expense documentation. A “fraudulent return” includes a return in which the individual is attempting to file using someone else’s name or SSN on the return or the taxpayer is presenting documents or information that have no basis in fact. A potentially abusive return is a return that the taxpayer is required to file but contains inaccurate information that may lead to an understatement of a liability or the overstatement of a credit resulting in a refund to which the taxpayer may not be entitled.

An ERO that is also a tax return preparer should exercise due diligence in the preparation of returns involving the Earned Income Tax Credit (EITC), as it is a popular target for fraud and abuse. Section 6695(g) of the Internal Revenue Code requires paid preparers to exercise due diligence in the preparation of returns claiming the head of

household filing status or certain credits including the EITC. Paid preparers must complete all required worksheets and meet all record keeping requirements.

## Verifying Taxpayer Identity and Taxpayer Identification Numbers (TINs)

To safeguard IRS *e-file* from fraud and abuse, an ERO should confirm identities and SSNs, Adoption Taxpayer Identification Numbers (ATINs) and Individual Taxpayer Identification Numbers (ITINs) of taxpayers, spouses and dependents listed on returns prepared by its firm. To prevent filing returns with stolen identities, an ERO should ask taxpayers not known to them to provide two forms of identification (photo IDs are preferable) that include the taxpayer's name and current or recent address. Also, seeing Social Security cards, ITIN letters and other documents for taxpayers, spouses and dependents avoids

including incorrect TINs on returns. Providers should take care to ensure that they transcribe all TINs correctly.

The TIN entered in the Form W-2, Wage and Tax Statement, in the electronic return record must be identical to the TIN on the version provided by the taxpayer. The TIN on the Form W-2 should be identical to the TIN on the electronic return unless otherwise allowed by the IRS. The IRS requires taxpayers filing tax returns using an ITIN to include the TIN, usually a SSN, shown on Form W-2 from the employer in the electronic record of the Form W-2. This may create an identification number (ITIN/SSN) mismatch as taxpayers must use their correct ITIN as their identifying number in the individual income tax return. The IRS *e-file* system can accept returns with this identification number mismatch. EROs should enter the TIN/SSN in the electronic record of the Form W-2 provided to them by taxpayers. Software

must require the manual key entry of the TIN as it appears on Form W-2 reporting wages for taxpayers with ITINs. EROs should ascertain that the software they use does not auto-populate the ITIN in the Form-W-2 and if necessary, replace the ITIN with the SSN on the Form W-2 the taxpayer provided.

Incorrect TINs, using the same TIN on more than one return or associating the wrong name with a TIN are some of the most common causes of rejected returns (see "**Acknowledgments of Transmitted Return Data**").

Additionally, Name Control and TINs identify taxpayers, spouses and dependents. A Name Control is the first four significant letters of an individual taxpayer's last name or a business name as recorded by the Social Security Administration (SSA) or the IRS. Having the wrong Name Control in the electronic return record for a taxpayer's TIN contributes to a large portion of TIN related rejects. The most

common example for a return rejecting due to a mismatch between a taxpayer's TIN and Name Control involves newly married taxpayers. Typically, the taxpayer may file using a correct SSN along with the name used in the marriage, but the taxpayer has failed to update the records with the SSA to reflect a name change. To minimize TIN related rejects, it is important to verify taxpayer TINs and Name Control information prior to submitting electronic return data to the IRS.

## Be Aware of Non-Standard Information Returns and Documents

The IRS has identified questionable Forms W-2 as a key indicator of potentially abusive and fraudulent returns. Be on the lookout for suspicious or altered Forms W-2, W-2G, 1099-R and forged or fabricated documents. EROs must always enter the non-standard form code in the electronic record of

individual income tax returns for Forms W-2, W-2G or 1099-R that are altered, handwritten or typed. An alteration includes any pen-and-ink change. Providers must never alter the information after the taxpayer has given the forms to them.

Providers should report questionable Forms W-2 if they see or become aware of them.

## Be Careful with Addresses

Addresses on Forms W-2, W-2G or 1099-R; Schedule C; or on other tax forms supplied by the taxpayer that differ from the taxpayer's current address must be input into the electronic record of the return. Providers must input addresses that differ from the taxpayer's current address even if the addresses are old or if the taxpayer has moved. EROs should inform taxpayers that, when the return is processed, the IRS uses the address on the first page of the return to update the taxpayer's address of record. The

IRS uses a taxpayer's address of record for various notices that it is required to send to a taxpayer's "last known address" under the Internal Revenue Code and for refunds of overpayments of tax (unless otherwise specifically directed by taxpayers, such as by Direct Deposit).

Providers must never put their address in fields reserved for taxpayers' addresses in the electronic return record or on Form 8453, U.S. Individual Income Tax Transmittal for an IRS *e-file* Return. The only exceptions are if the Provider is the taxpayer or the power of attorney for the taxpayer for the tax return.

## Avoiding Refund Delays

EROs should advise taxpayers that they can avoid refund delays by having all their taxes and obligations, such as child support and student loan debt, paid, providing current and correct information to the ERO, ensuring that all bank account information is up to date,

ensuring that their Social Security Administration records are current and carefully checking their tax return information before signing the return.

EROs can do many things for clients and customers to avoid rejects and refund delays. Here are some suggestions:

- Require documentation of social security and other identification numbers and associated names for all taxpayers and dependents;
- Exercise care in the entry of tax return data into tax return preparation software and carefully check the tax return information before signing the tax return;
- Confirm that any ITINs reported on the return haven’t expired due to non-use or under the announced IRS schedule;

- Review information provided and don’t submit returns claiming false items on tax returns or present altered or suspicious documents;
- Ask taxpayers if there were problems with last year’s refund; if so, see if the conditions that caused the problems have been corrected or can be avoided this year;
- Track client issues that result in refund delays and analyze for common problems; counsel taxpayers on ways to address these problems.

## Refund Returns

When taxpayers are entitled to refunds, Providers should inform them that they have several options. An individual income tax refund may be applied to next year’s estimated tax, received as a Direct Deposit or paper check or be split so that a portion is applied to next year’s estimated tax and the

rest received as a Direct Deposit or paper check.

Providers must not direct the payment (or accept payment) of any monies issued to a taxpayer client by the government in respect of a Federal tax liability to the Provider or any firm or entity with which the Provider is associated. The IRS may sanction Providers and individuals who direct or accept such payment.

When filing and/or printing a paper return, Software Developers are being asked to default the “Routing Transit and Account Numbers” in the software packages on Forms 1040/1040SR/1040NR/1040SSPR, with all capital X’s, when taxpayers choose not to have their refund directly deposited. These fields should never be blank on paper filed returns.

# Direct Deposit of Refunds

Taxpayers often elect the Direct Deposit option because it is the fastest way of receiving refunds. Providers must accept any Direct Deposit election to qualified accounts in the taxpayer's name at any eligible financial institution designated by the taxpayer. Amended Forms 1040 and 1040-SR Returns (with attached 1040-X) resulting in a refund are not yet eligible for direct deposits. Qualified accounts include savings, checking, share draft or consumer asset accounts (for example, IRA or money market accounts). Taxpayers should not request a deposit of their refund to an account that isn't in their own name (such as their tax return preparer's own account). The taxpayer may not designate refunds for Direct Deposit to credit card accounts.

Qualified accounts are accounts held by financial institutions within the United States and established primarily for personal, family

or household purposes. Qualifying institutions may be national banks, state banks (including the District of Columbia and political sub-divisions of the 50 states), savings and loan associations, mutual savings banks and credit unions.

By completing **Form 8888, Allocation of Refund (Including Savings Bond Purchases)**, the taxpayer may split refunds between up to three qualified accounts. A qualified account can be a checking, savings or other account such as an individual retirement arrangement (IRA), health savings account (HSA), Archer MSA, Coverdell education savings account (ESA) or TreasuryDirect online account. The taxpayer may also buy up to $5,000 in U. S. Series I Bonds. For example, a taxpayer expecting a refund of $400 may choose to deposit $150 into a checking account, $150 into a savings account and $100 into an IRA account. Taxpayers may choose the refund splitting

option regardless of which Form 1040 series tax form they file.

Providers should caution taxpayers that some financial institutions do not permit the deposit of tax refunds into an account opened in someone else's name, the deposit of joint individual income tax refunds into individual accounts or the deposit of tax refunds into check or share draft accounts that are "payable through" another institution. Taxpayers should verify their financial institution's Direct Deposit policy before they elect the Direct Deposit option. The IRS isn't responsible if the financial institution refuses Direct Deposit for this reason.

Taxpayers who choose Direct Deposit must provide Providers with account numbers and routing transit numbers for qualified accounts. The IRS tax return instructions show how to find and identify these numbers. The taxpayer can best obtain this information from official financial institution records,

account cards, checks or share drafts that contain the taxpayer's name and address. The sole exception involves accounts specifically created to receive refunds that repay refund products offered by financial institutions. In those cases, Providers may supply the identifying account data.

To combat fraud and identity theft, the IRS limits the number of refunds electronically deposited into a single financial account or pre-paid debit card to three. The fourth and subsequent refunds automatically will convert to a paper refund check and be mailed to the taxpayer.

Providers with repeat customers or clients should check to see if taxpayers have new accounts. Some software stores prior year's information and reuses it unless it is changed. If account information isn't current, taxpayers do not receive Direct Deposit of their refunds.

Providers must advise taxpayers that they can't cancel a Direct Deposit election or make

changes to routing transit numbers of financial institutions or to their account numbers after the IRS has accepted the return. Providers must not alter the Direct Deposit information in the electronic record after taxpayers have signed the tax return.

> **Note:** Providers must never charge a separate fee for Direct Deposit.

Refunds that are not direct deposited because of institutional refusal, wrong account or routing transit numbers, closed accounts, bank mergers or any other reason are issued as paper checks, resulting in refund delays of up to ten weeks. While the IRS ordinarily processes a request for Direct Deposit, it reserves the right to issue a paper check and does not guarantee a specific date for deposit of the refund into the taxpayer's account.

Treasury's Bureau of the Fiscal Service issues federal income tax refunds. Neither the IRS nor Fiscal Service is responsible for the misapplication of a Direct Deposit that results

from error, negligence or malfeasance on the part of the taxpayer, the Provider, financial institution or any of their agents.

## Payment Options for Taxpayers

Taxpayers who owe additional tax must pay the taxes they owe by the original due date of the return or be subject to interest and penalties. An extension of time to file may be filed electronically by the original return due date, but it is an extension of time to file the return, not an extension of time to pay. Providers should inform taxpayers of their obligations and options for paying balances due. Taxpayers have several options when paying taxes.

### Electronic Funds Withdrawal

Taxpayers can e-file and, at the same time, authorize an electronic funds withdrawal (EFW). Taxpayers who choose this option must provide account numbers and routing transit numbers for qualified savings,

checking or share draft accounts to the Provider. The IRS tax return instructions describe how to find and identify these numbers. Providers should encourage their clients to confirm their account numbers and routing transit numbers with their financial institution. If a financial institution is unable to locate or match the numbers entered in a payment record with account information they have on file for a given taxpayer, they reject (return) the direct debit request.

Providers should caution taxpayers to ensure, before they e-file, that their financial institution allows EFW requests from the designated account. Some credit unions do not allow direct debits from share accounts.

Taxpayers can schedule a payment for withdrawal on a future date. Scheduled payments must be effective on or before the return due date. For example, the Provider may transmit an individual income tax return in March and the taxpayer can specify that

the withdrawal be made on any day on or before the return due date. The taxpayer does not have to remember to do anything later. For returns transmitted after the due date, the payment date must be the same as the date the Provider transmitted the return. The taxpayer must authorize EFW payments by completion of a payment record at the time the balance due return or other form is e-filed.

Taxpayers can make payments by EFW for the following:

- Current year – Form 1040 series return.
- **Form 4868, Application for Automatic Extension of Time to File U.S. Individual Income Tax Return**.
- **Form 2350, Application for Extension of Time to File U.S. Income Tax Return**

- **Form 1040-ES, Estimated Tax for Individuals.** Taxpayers can make up to four advance quarterly estimated tax payments at the same time that they electronically file the Form 1040 series return. For example, four Form 1040-ES quarterly tax payments for tax year 2023 may be submitted with the electronic filing of the taxpayer's tax return for tax year 2022.

Providers should be careful to ensure that all the information needed for the EFW request is included with the return. The payment record must include the following:

- Routing Transit Number (RTN);
- Bank account number;
- Type of account (checking or savings);
- Requested payment date (i.e., YYYYMMDD); and

- Amount of tax payment for balance due payments sent after the due date; this amount may include interest and penalty payment.

If taxpayers do not provide all the needed information, Providers must contact the taxpayers. If the Provider is unsuccessful in obtaining or transmitting the EFW information, but the return is otherwise complete, the Provider should proceed with the origination of the electronic return data to the IRS. The Provider must inform their clients that they need to make other arrangements to pay the balance due and/or estimated payments. See below for other payment options.

## IRS Direct Pay

With this secure online service, taxpayers can pay their individual tax bill or estimated tax payments directly from their checking or savings account at no cost. They will receive

instant confirmation after they submit their payment.

Taxpayers can make payments with IRS Direct Pay for the following:

- Current and prior year Form 1040 series returns
- Installment agreements
- Form 1040–ES (estimated tax for individuals)
- Form 4868 (extension payments)

More options are available at **IRS.gov/payments**.

## Credit or Debit Card Payments

Taxpayers can make credit or debit card payments when e-filing or separately online or by phone.

- Integrated e-file and e-pay: Taxpayers can e-file and pay their balance at the same time by debit or credit card if the

tax software used includes this option. The software prompts taxpayers to enter the necessary card information. The service provider charges taxpayer's convenience fees based on the amount of the tax payment and informs them of these fees before taxpayers authorize the payments.

- Online by Phone: Taxpayers may pay online at **IRS.gov/payments** or by phone, credit or ATM/debit card (American Express® Card, Discover® Card, MasterCard® or Visa® card) and NYCE®, PULSE® or STAR® logos. This service is available through credit card service providers. The service provider charges a convenience fee based on the amount of the tax payment. The software informs taxpayers of this fee during the transaction, and they can choose to end the transaction before the payment is completed and

confirmed. The software provides a confirmation number at the end of the transaction. EROs should inform taxpayers of this option and tell them that fees may vary between service providers.

Further detailed information on payment options is available on **IRS.gov/payments**.

## Electronic Federal Tax Payment System (EFTPS)

Individual taxpayers, who make more than one tax payment per year, particularly installment or Form 1040 estimated payments, find EFTPS very convenient. Taxpayers can enroll in EFTPS via the Internet at EFTPS.gov or by completing **Form 9783, Electronic Federal Tax Payment System Individual Enrollment** and mailing it to the EFTPS Enrollment Center. After EFTPS processes the enrollment, taxpayers receive two separate mailings. One is a Confirmation/

Update Form. The other is a letter that includes the taxpayers' Enrollment Trace Number, Personal Identification Number (PIN) and instructions on how to obtain an Internet Password. Once taxpayers receive the PINs, they may begin making payments by phone. After the taxpayers obtain their Internet Password, they may begin making payments via the Internet. With EFTPS, taxpayers only need to enroll once to make a payment by both telephone and the Internet as the payment methods are interchangeable. Payments can be made 24/7; however, taxpayers must submit their tax payment instructions to EFTPS before 8:00 p.m. ET at least one calendar day prior to the tax due date. Taxpayers can schedule individual tax payments up to 365 days in advance.

## Pay with Cash

For taxpayers who are unbanked there is a cash option. Individuals wishing to take advantage of this payment option should visit

the **IRS.gov/payments** page, select the **cash** option in the other ways you can pay section and follow the instructions.

## Pay by Check or Money Order

Taxpayers may pay the balance due by mailing a check accompanied by **Form 1040-V, Payment Voucher**. Providers must supply Form 1040-V to taxpayers, if needed, and help them identify the correct mailing address from the chart on the back of the form. Taxpayers do not have to mail these vouchers at the same time the Provider transmits the electronic return. For example, the return may be transmitted in January and the taxpayer may mail the payment and voucher at any time on or before the return due date. Further detailed information on paying by check or money order is available on the **IRS.gov/payments** page by selecting the **check or money order** option in the other ways you can pay section.

## Installment Agreement

Taxpayers who can't pay the amount they owe for Form 1040 series returns and owe $50,000 or less in combined taxes, interest and penalties may use the **Online Payment Agreement (OPA)** application to request a payment plan (installment agreement). Authorized representatives with a power of attorney may use OPA on the taxpayer's behalf. OPA will result in immediate notification of whether the payment plan is approved. Alternatively, they can submit **Form 9465, Installment Agreement Request**, to the IRS by mail. The Provider can transmit Form 9465 electronically (if supported by software) with the taxpayer's electronic return data, or the form may be submitted later by mail. It may take 30 days or more for a response to Form 9465, regardless of how it is submitted. If the installment agreement is accepted, the IRS charges a user fee, which may be waived or

reimbursed for low-income taxpayers. Taxpayers who apply through OPA are charged a lower user fee, and an even lower user fee if they use the direct debit payment option.

## Signing an Electronic Tax Return

As with an income tax return submitted to the IRS on paper, the taxpayer and paid tax return preparer (if applicable) must sign an electronic income tax return. Taxpayers must sign individual income tax returns electronically. There are currently two methods for signing individual income tax returns electronically (see **Electronic Signature Methods**).

Taxpayers must sign and date the Declaration of Taxpayer to authorize the origination of the electronic submission of the return to the IRS prior to the transmission of the return to IRS. The Declaration of Taxpayer includes the taxpayers' declaration under penalties of

perjury that the return is true, correct and complete, as well as the taxpayers' Consent to Disclosure. The Consent to Disclosure authorizes the IRS to disclose information to the taxpayers' Providers. Taxpayers authorize Intermediate Service Providers, Transmitters and EROs to receive from the IRS an acknowledgment of receipt or reason for rejection of the electronic return, the reason for any delay in processing the return or refund and the date of the refund.

Taxpayers must sign a new declaration if the electronic return data on individual income tax returns is changed after taxpayers signed the Declaration of Taxpayer and the amounts differ by more than either (i) $50 to "Total income" or "AGI," or (ii) $14 to "Total tax," "Federal income tax withheld," "Refund" or "Amount you owe."

## Electronic Signature Methods

There are two methods of signing individual income tax returns with an electronic signature available for use by taxpayers. Both the Self-Select PIN and Practitioner PIN methods allow taxpayers to use a Personal Identification Number (PIN) to sign the return and the Declaration of Taxpayer.

The Self-Select PIN method requires taxpayers to provide their prior year Adjusted Gross Income (AGI) amount or prior year PIN for use by the IRS to authenticate the taxpayers. EROs should encourage taxpayers who do not have their original prior year AGI or PIN to call IRS Tax Help at 800-829-1040.

This method may be completely paperless if the taxpayers enter their own PINs directly into the electronic return record using keystrokes after reviewing the completed return. Taxpayers may also authorize EROs to enter PINs on their behalf, in which case the

taxpayers must review and sign a completed signature authorization form after reviewing the return. Also see **IRS e-file Signature Authorization (Forms 8878 and 8879)**.

The Practitioner PIN method does not require the taxpayer to provide their prior year AGI amount or prior year PIN. Instead, taxpayers must always sign a completed signature authorization form (see **IRS e-file Signature Authorization (Forms 8878 and 8879)**). Taxpayers who use the Practitioner PIN method must sign the signature authorization form even if they enter their own PINs in the electronic return record using keystrokes after reviewing the completed return.

Regardless of the method of electronic signature used, taxpayers may enter their own PINs;

EROs may select and enter the taxpayers' PINs; or the software may generate the taxpayers' PINs in the electronic return. After reviewing the return, the taxpayers must

agree by signing an IRS *e-file* Signature Authorization containing the PIN.

The following taxpayers are ineligible to sign individual income tax returns with an electronic signature using the Self-Select PIN:

- Primary taxpayers under age sixteen who have never filed; and
- Secondary taxpayers under age sixteen who didn't file the prior tax year.

EROs should recommend that taxpayers keep a copy of their completed tax return to assist with authentication in the subsequent year.

## IRS *e-file* Signature Authorization (Forms 8878 and 8879)

Anytime an ERO enters the taxpayer's PIN on the electronic return, the ERO must, prior to submission of the return, complete an IRS *e-file* Signature Authorization form which must be signed by the taxpayer. **Form 8879, IRS**

***e-file* Signature Authorization**, authorizes an ERO to enter taxpayers' PINs on individual income tax returns and **Form 8878, IRS *e-file* Authorization for Form 4868 or Form 2350**, authorizes an ERO to enter taxpayers' PINs on Form 1040 extension forms. The ERO must keep Forms 8878 and 8879 for three years from the return due date or the IRS received date, whichever is later. EROs must not send Forms 8878 and 8879 to the IRS unless the IRS requests they do so.

> **Note:** Form 8878 is only needed for Forms 4868 when taxpayers are authorizing an electronic funds withdrawal and want an ERO to enter their PINs.

The ERO may enter the taxpayers' PINs in the electronic return record before the taxpayers sign Form 8878 or 8879, but the taxpayers must sign and date the appropriate form before the ERO originates the electronic submission of the return (or extension form).

The taxpayer must sign and date the Form 8878 or Form 8879 after reviewing the return and ensuring the tax return information on the form matches the information on the return. The taxpayer may return the completed Form 8878 or Form 8879 to the ERO by hand delivery, U.S. mail, private delivery service, fax, email or an Internet website.

Only taxpayers who provide a completed tax return to an ERO for electronic filing may sign the IRS *e-file* Signature Authorization without reviewing the return originated by the ERO. The ERO must enter the line items from the paper return on the applicable Form 8878 or Form 8879 prior to the taxpayers signing and dating the form. The ERO may use these pre-signed authorizations as authority to input the taxpayer's PIN only if the information on the electronic version of the tax return agrees with the entries from the paper return.

## Electronic Signature Guidance for Forms 8878 and 8879

Taxpayers have the choice of using electronic signatures for Forms 8878 and 8879 if the software provides the electronic signature capability. If taxpayers use an electronic signature, the software and the Electronic Return Originator (ERO) must meet certain requirements for verifying the taxpayer's identity.

Electronic signatures appear in many forms and may be created by many different technologies. No specific technology is required. Examples of currently acceptable electronic signature methods include:

- A handwritten signature input onto an electronic signature pad.
- A handwritten signature, mark or command input on a display screen by a stylus device.

- A digitized image of a handwritten signature that is attached to an electronic record.
- A typed name (e.g., typed at the end of an electronic record or typed into a signature block on a website form by a signer).
- A shared secret (e.g., a secret code, password or PIN) used by a person to sign the electronic record.
- A digital signature.
- A mark captured as a scalable graphic.

The software must record the following data:

- Digital image of the signed form.
- Date and time of the signature.
- Taxpayer’s computer IP address (Remote transaction only).
- Taxpayer’s login identification – user name (Remote transaction only).

- Identity verification: taxpayer's passed results of knowledge-based authentication, and for in-person transactions, confirmation that government photo identification has been verified.
- Method used to sign the record (e.g., typed name); or a system log; or other audit trail that reflects the completion of the electronic signature process by the signer.

**Note:** The ERO must provide this information to the IRS upon request.

## Digital Identity Verification Requirements

The electronic signing process must be associated with a person, and accordingly, ensuring the validity of any electronically signed record begins with identification and authentication of the taxpayer. The electronic signature process must be able to generate

evidence of the person the electronic form of signature belongs to, as well as generate evidence that the identified person is associated with the electronic record.

If there is more than one taxpayer for the electronic record, the electronic signature process must be designed to separately identify and authenticate each taxpayer.

The identity verification requirements must be in accordance with National Institute of Standards and Technology, Special Publication 800-63, Electronic Authentication Guideline, Level 2 assurance level and knowledge-based authentication or higher assurance level.

## Electronic Signature Via In-Person Transaction

An in-person transaction for electronic signature is one in which the taxpayer is electronically signing the form and the ERO is physically present with the taxpayer. The ERO

must confirm the taxpayer's identity for in-person transactions unless there is a multi-year business relationship. A multi-year business relationship is one in which the ERO has originated tax returns for the taxpayer for a prior tax year and has identified the taxpayer using the identity verification process described below.

For in-person transactions, the ERO must inspect a valid government photo identification; compare photo to the taxpayer and record the name, social security number, address and date of birth. Examples of government photo identification (ID) include a driver's license, employer ID, school ID, state ID, military ID, national ID, voter ID, visa or passport.

Verify that the name, social security number or Individual Taxpayer Identification Number (ITIN), address, date of birth and other personal information on record are consistent with the information provided through record

checks with the applicable agency or institution or through credit bureaus or similar databases. For in-person transactions, the identity verification through a record check is optional.

## Electronic Signature Via Remote Transaction

A remote transaction for electronic signature is one in which the taxpayer is electronically signing the form and the ERO isn’t physically present with the taxpayer. For remote transactions, the ERO must record the name, social security number, address and date of birth.

Verify that the name, social security number, address, date of birth and other personal information on record are consistent with the information provided through record checks with the applicable agency or institution or through credit bureaus or similar databases.

**Note:** An electronic signature via remote transaction does not include handwritten signatures on Forms 8878 or 8879 sent to the ERO by hand delivery, U.S. mail, private delivery service, fax, email or an Internet website.

## Identity Verification

The software used for the electronic signature process may use credit records, also known as credit reports, to verify the taxpayer's identity. Identity verification may consist of a record check with a credit reporting company. A credit reporting company uses information from the taxpayer's credit report to generate knowledge-based authentication questions. This action may create an entry on the credit report called a "soft inquiry."

The software used for the electronic signature process should include an advisory to taxpayers stating the use of third-party data

for identity verification; how third-party data is used for identity verification; if a "soft inquiry" will be generated and the effect, if any, on the credit report, credit scores and reporting to lenders; and how the inquiry may appear on the credit report.

The software should also include an advisory to taxpayers stating the IRS won't be given view of or access to a taxpayer's credit report, nor will the credit reporting company or other identity verification third party have access to the taxpayer's tax information.

The process of identity verification using a record check with a credit reporting company or other identity verification third party for purposes of electronically signing does not require additional consents from the taxpayer beyond those obtained for preparing and filing their taxes; nor does it violate the provisions of Internal Revenue Code section 7216 or its regulations.

## Identity Verification Failure

The software will enable the identity verification using knowledge-based authentication questions when an ERO uses tax preparation software to interact with the taxpayer for purposes of obtaining an electronic signature on Form 8878 or 8879. If the taxpayer fails the knowledge-based authentication questions after three attempts, then the ERO must obtain a handwritten signature on Form 8878 or 8879.

## Electronic Records

Electronic signatures must be linked to their respective electronic records to ensure that the signatures can’t be excised, copied or otherwise transferred to falsify an electronic record.

After the electronic record has been signed, it must be tamper-proof. Therefore, techniques must be employed that lock a document and prevent it from being changed. Storage

systems must have secure access control to ensure that the electronic records can’t be changed.

Additionally, storage systems must also have a retrieval system that includes an indexing system, and the ability to reproduce legible and readable hardcopies of electronically stored records.

## Electronic Signatures for EROs

EROs must also sign with a PIN. EROs should use the same PINs for the entire tax year. The ERO may manually input, or the software can generate the PIN in the electronic record in the location designated for the ERO Electronic Filing Identification Number (EFIN)/PIN. The ERO is attesting to the ERO Declaration by entering a PIN in the ERO EFIN/PIN field. For returns prepared by the ERO firm, return preparers are declaring under the penalties of perjury that they

reviewed the returns, and they are true, correct and complete.

EROs may authorize members of their firms or designated employees to sign for them, but the EROs are still responsible for all the electronic returns originated by their firms.

For returns prepared by other than the ERO firm that originates the electronic submission, the ERO attests that the return preparer signed the copy of the return and that the electronic return contains tax information identical to that contained in the paper return.

The ERO must enter the return preparer's identifying information (name, address, EIN, and PTIN) in the electronic return.

EROs may sign **Form 8878** and **Form 8879** by rubber stamp, mechanical device (such as signature pen) or computer software program as described in **Notice 2007-79**.

The signature must include either a facsimile of the individual ERO’s signature or of the ERO’s printed name. EROs using one of these alternative means are personally responsible for affixing their signatures to returns or requests for extension. This does not alter the requirement that taxpayers must sign Form 8878 and Form 8879 by a handwritten or electronic signature.

The ERO must keep Forms 8878 and 8879 for three years from the return due date or the IRS received date, whichever is later. EROs must not send Forms 8878 and 8879 to the IRS unless the IRS requests they do so.

# Submitting the Electronic Return to the IRS

Once signed, an ERO must originate the electronic submission of a return as soon as possible. EROs must not electronically file individual income tax returns prior to receiving Forms **W-2, Wage and Tax Statement, W-2G, Certain Gambling Winnings or 1099-R, Distributions from Pensions, Annuities, Retirement or Profit-Sharing Plans, IRAs, Insurance Contracts, etc.** If the taxpayer is unable to secure and provide a correct Form **W-2**, **W-2G**, or **1099-R**, the ERO may electronically file the return after the taxpayer completes **Form 4852, Substitute for Form W-2, Wage and Tax Statement or 1099-R, Distributions from Pensions, Annuities, Retirement or Profit-Sharing Plans, IRAs, Insurance Contracts, etc.**, in accordance with the use of that form. If Form 4852 is used, the nonstandard W-2 indicator must be

included in the record, and the ERO must maintain Form 4852 in the same manner required for Forms W-2, W-2G and 1099-R.

An ERO must ensure that stockpiling of returns does not occur at its offices. Stockpiling is:

- collecting returns from taxpayers or from another Authorized IRS *e-file* Provider prior to official acceptance in IRS *e-file*; or
- after official acceptance to participate in IRS *e-file*, stockpiling refers to waiting more than three calendar days to submit the return to the IRS once the ERO has all necessary information for origination.

The IRS does not consider as stockpiled current filing year returns held prior to the date the IRS accepts transmission of electronic returns. EROs must tell taxpayers that it can’t transmit returns to the IRS until

the date the IRS accepts transmission of electronic returns. Although holding late returns during periods when IRS electronic filing isn't available isn't stockpiling, Providers should mail the returns to the IRS mailing addresses in the form's instructions.

## Internet Protocol Information

Internet Protocol (IP) information of the computer the ERO uses to prepare the return (or originate the electronic submission of collected returns) must be included in all individual income tax returns. The required Internet Protocol information includes:

- Public/routable IP address
- IP date
- IP time
- IP time zone

With many different ERO e-filing business models, the computer used to prepare (or originate the electronic submission of

collected returns) may not have a public/routable IP address. If the computer used for preparation (or origination of the electronic submission of collected returns) is on an internal reserved IP network, then the IP address should be the public/routable IP address of the computer used to submit the return. If the computer used for preparation (or origination of the electronic submission of collected returns) is used to transmit the return to the IRS, then the IP address should be the public/routable IP address of that computer. If it isn’t possible to capture the public/routable IP address, then the ERO or software may have to hard code the IP address into each return.

The IRS will reject individual income tax returns e-filed without the required IP address. Any return received by the IRS containing a private/non-routable IP address will be flagged in the acknowledgment File with an “R” in the Reserved IP Address Code

field of the ACK key record indicating that a reserved IP address is present for the return.

## Device ID

The IRS has implemented a Device ID field for electronic return filers and preparers. The IRS will use this unique identifier; in addition to key elements we already collect to improve fraud and ID theft detection. Vendors implementing Device ID in their software should ensure that their privacy notice will cover Device ID.