

Overview

Industry Trusted Customer Requirements

The industry, state and IRS partners recognize that even though fraud filings will still occur, we all must be proactive and take steps to reduce or prevent the fraud. The acceptance of username and passwords as the only source of authentication is no longer a viable solution and must be enhanced through minimum mandatory additional levels of authentication. Minimum requirements are established in cooperation with industry partners, states and the IRS to present a consistent standard for front-end customer identity authentication using recognized national standards from the National Institute of Standards and Technology (NIST) and the IRS Pub. 1075.

The IRS and States working with Industry partners have established the following minimum set of standards and methodology that Industry will use to help deter potential identity theft tax refund fraud activity, which going forward will be based on increasingly stringent and effective national standards and protocols. To preserve innovation and creativity, Industry partners may choose to, and are encouraged to, exceed the minimum standards established and conduct their own independent and unique analysis, based on patterns or trends they observe and identify. These minimum requirements will be reviewed and strengthened by July of each year.

Passwords:

Through the use of strong passwords and locking out an account after many consecutive failed attempts, the goal is to mitigate password guessing and brute force attacks. For the lockout feature, the working group established a number that industry supports while recognizing that, as stated in the NIST recommendations, “locking out an account after only a few failed attempts has a significant impact on legitimate users” and are targeting 10 as a reasonable starting point for this first year in lieu of another alternative of increasing the delay after each failed attempt. These standards also meet the IRS Pub 1075 requirements.

Out-of-Band Verification:

Tax agencies recognize that out-of-band verification is becoming a national standard and recommend that the industry partners implement this protocol. The IRS recently incorporated this standard for its “Get Transcript” application. Because not all industry partners will implement this verification protocol for this upcoming processing season, the working group also identified a data element to be submitted with each return to identify the ability to verify the customer’s email address. The tax agencies will also include a question within their annual filing agreements to determine if the industry partner will implement out-of-band verification.

Requirements Not Prescriptive:

It would not be wise for government to provide very detailed prescriptive requirements and in so doing possibly curtail the ability of the tax software industry to exceed the current critical need for “knowing your customer”, but the steps outlined are a baseline. The document is formatted to provide clarity to the minimum requirements baseline recognized in current national standards as agreed upon by the working group. Industry will meet the

requirements set forth in this document based on their particular business models and if an industry partner addresses identity authentication using other features not identified in these minimum requirements, the industry partner will work directly with each tax agency to identify the protocol and gain the agency's approval. The government will not dictate specifically how these standards are met and the vendor ultimately must establish that the e-filing application meets or exceeds the minimum requirements.

Initial Target Audience

The initial target population of providers is all do-it-yourself taxpayer interfaces into an on-line tax system including (but not limited to):

- When the data is stored electronically online or
- When the customer establishes an online account

Establishing a trusted customer requirement for this target audience is an important step in building a robust tax filing system that:

- Follows nationally recognized standards for implementing "Knowing Your Customer" identity authentication
- Ensures consistent minimum requirements are established for industry to efficiently support multiple tax agencies
- Mitigates the potential for account takeovers
- Reduces the opportunity for fraudulent return filing
- Establishes a process to verify identity in future interactions including but not limited to password changes
- Enhances security / protection measures for taxpayer confidential and sensitive information
- Increases the public confidence and trust in the tax filing system

These steps will be accompanied by national and local messaging driving home these principles. Note that these requirements can and will change over time to respond to new technologies and new threats.

Minimum Requirements for Identity Authentication

The following minimum requirements for the target audience will be incorporated in agency e-filing agreements for certification and will be verified by optional post-launch reviews.

New Customer Standard

- I. Username – no specific format requirement
 1. Include helpful tips – such as do not use email address, SSN, First and Last Name, etc.
- II. Password
 1. All customers will be provided messaging on the importance of a strong password (at least 8 characters, upper, lower case, digit and special char) as an important step for protecting their identity.
 2. Implement a 15 minute interval after lockout feature with no more than 10 unsuccessful login attempts
 3. At least 8 characters
 - Including **all** of the following:
 - At least 1 uppercase character (A-Z)
 - At least 1 lowercase character (a-z)
 - At least 1 digit (0-9)
 - At least 1 special character (punctuation)
- III. Three security questions (If the company does not support out-of-band and will be using the security questions as one of the choices in the minimum “Returning Customer Standards” below)
 1. Question and answer provided by the customer or established by industry
 2. Do not use questions that have readily available answers
 3. Do not use questions that have answers that are shared with others or are available to others
- IV. Customer is required to enter an email address
- V. Customer is provided an option to enter a cell phone number
- VI. Email Address Verification (see Filing Expectations)
 1. The preferred method is for industry partners to implement out-of-band verification.
 - a. Out-of-band verification is sending an email or text to the customer with a PIN. Through a user interface, the customer enters a PIN which is validated through the software before allowing the customer to continue with the process.
 2. If an industry partner does not implement out-of-band for New Customers, the industry partner must make their best effort to verify the email address.

Returning Customer Standard

For Processing Year 2016, Industry will:

- Provide messaging to all returning customers on the importance of a strong password (at least 8 characters, upper, lower case, digit and special char) and given the opportunity to change their password as an important step for protecting their identity;
- Implement a 15 minute interval after lockout feature with no more than 10 unsuccessful login attempts;
- Ensure that the customer has previously entered an email address;
- Ensure that the customer has the opportunity to add a cell phone entry.

I. Is the IP address or device ID recognized from previous login?

- If yes, continue to next step.
- If no, successful completion of one of the following is required before proceeding:

1. Out-of-band verification or
2. Answer randomly selected security question

II. Do the security questions on record meet the New Customer standards? (Not applicable if the company is choosing to use alternate authentication methods based on the below options, and such authentication is successful.)

- If yes, continue to next step
- If no,
 1. Customer must update security questions to meet the New Customer standard

III. Is the customer indicating they have a new email address?

- To change an email address, customer must successfully complete one of the following:
 1. Out-of-band verification to email or cell phone with a notification sent to the old email address or cell with instructions on what to do if they didn't change their email address or
 2. Answer randomly selected security question

IV. Has there been account activity within 90 days?

- If yes, continue to next step
- If no, AND the customer is NOT using a trusted/proven device or IP Address, successful completion of one of the following is required before proceeding:
 1. Out-of-band verification or
 2. Answer randomly selected security question

V. In cases of increased system risk based on identified facts and circumstances determined collaboratively by industry, agencies and IRS (needs to be flexible):

Customers may be required to successfully complete one of the following before proceeding:

1. Out-of-band verification or
2. Answer randomly selected security question

VI. Prior to filing, Industry will complete Email Address Verification (see Filing Expectations)

1. The preferred method is for industry partners to implement out-of-band verification.
 - a. Out-of-band verification is sending an email or text to the customer with a PIN. Through a user interface, the customer enters the PIN, which is validated through the software before allowing the customer to continue with the process.
2. If an industry partner does not implement out-of-band for New Customers, the industry partner must make their best effort to verify the email address.

Filing Expectations

- Determine if more than one account is using a Primary and/or Secondary SSN,
 - If the SSN is used in multiple accounts, at least one of the following actions must apply to all related accounts:
 - Notify account holder(s) that the Primary and/or Secondary SSN is used within another account OR
 - Notify account holder(s) that the Primary and/or Secondary SSN is used within another account AND Implement Additional Authentication measures prior to filing to validate the authenticity of one or more of the related accounts
 - All account holders have the opportunity to report the situation to the right authorities if they suspect improper use of the SSN.
- A data element provided by the vendor will be used to indicate the level of email verification performed for each filed return. Tax agencies may request acknowledgement of the use of out-of-band within the e-filing agreement (see Agreement Statements) and may use out-of-band capability and the indicators in the process of examining the internal analytics of the return.
- The following schema data element indicators will be used to report the level of contact verification that occurred during the filing process:
 - Email Address Verification (Element name Email_Address_Ind)
 - 0 = Can't send email
 - 1 = Bounced email
 - 2 = Delivered email – one-way
 - 3 = Successful out-of-band (text or email)
- To reduce the occurrences of multiple fraudulent returns, Industry will ensure that, at the point of filing, there are no more than two resident state returns filed with a single federal return.

Agreement Statements

In order to assist with fraud detection and prevention, the Idaho State Tax Commission requests information about the business practices of our vendor partners.

- 1. Do you use out-of-band verification practices for your customer verification process?
 - a. Out-of-band verification is sending an email or text to the customer with a PIN. Through a user interface, the customer enters the PIN, which is validated through the software before allowing the customer to continue with the process.
_____ Yes _____ No

- 2. Do you meet nationally recognized standards for implementing identity authentication by using:
 - a. The standards identified in the Identity Authentication section of this agreement.
 - b. An equivalent standard for identity authentication that meets or exceeds the minimum requirements. Please describe your proposed process for agency review.
_____ a. _____ b. Description _____

- 3. Do you agree to add “consent to disclosure” language, such as outlined on page 8, relating to certain characteristics of use of the system, to your user agreement?
_____ Yes _____ No

(name)

(signature)

(date)

In this section, “tax services provider” is defined as a:

Electronic Return Originator (ERO): An ERO originates the electronic submission of a tax return through IRS or state *e-file* after the taxpayer authorizes the electronic filing of the return.

Online Filing Provider: An Online Filing Provider allows taxpayers to self-prepare returns by entering return data directly into commercially available software downloaded from an Internet site and prepared off-line, or through an online Internet site, or loaded from physical media onto a desktop computer or mobile device.

Software Developer: An Authorized IRS or state e-file Provider that develops software for the purposes of (a) formatting the electronic portions of returns according to Publication 4164 or state specifications and/or (b) transmitting the electronic portion of returns directly to the IRS or the state. A Software Developer may also sell its software.

Transmitter: An Authorized IRS or state e-file Provider that transmits the electronic portion of a return directly to the IRS or the state. An entity that provides a “bump up” service is also a Transmitter. A bump up service provider increases the transmission rate or line speed of formatted or reformatted information that it is sending to the IRS or the state via a public switched telephone network.

A tax services provider may serve its customers in more than one of these roles.

A tax services provider may use any tax return information provided by a taxpayer, whether in and for the current year or for prior years, for the purpose of identifying a suspicious or potentially fraudulent return from or related to that taxpayer. For these purposes, tax return information means any and all documents or materials provided by the taxpayer or required by the taxing authority that the tax services provider uses in the course of the return preparation and submission.

Tax services providers shall produce analytic compilations of federal and state tax return and submission information that directly relate to the internal management or support of the tax services provider’s business, which shall include aggregated data compilations to identify potentially fraudulent behaviors or patterns. The analytic compilation shall employ any tax return information provided by the taxpayer.

Tax services providers shall disclose the compilations of tax information to Idaho through IRS secure data transmission on at least a weekly basis and identify by use of federal and state submission IDs any return the preparer believes is potentially fraudulent.

In addition, if a tax services provider has a bona fide belief that a particular individual’s activity, discovered by data mining a statistical compilation, violated criminal law, the tax services provider shall disclose that individual’s tax return information to the state of Idaho.

During the 2016 filing season, some of the new elements of information (possible fraud indicators) that providers will be collecting and submitting to the tax agency as a part of industry reporting are not in the return itself, but relate to certain characteristics of use of the system.

For this reason you may wish to re-visit the language in your taxpayer consent to disclosure. Suggested standard additional text to be included in the taxpayer consent is below.

In addition, by using a computer system and software to prepare and transmit my return electronically, I consent to the disclosure to the [state] of all information pertaining to my use of the system and software and to the transmission of my tax return electronically.

You may also wish to reference the identity theft language we are adding to our Individual Income Tax instructions booklet for T2015.

“How Identity Theft May Affect Your Tax Return”

Identity theft is affecting more people each year. From 2014 to 2015, there was a 64% increase in stolen identities used to file Idaho income tax returns. To help protect you and any refund you may be due, the Tax Commission uses multiple processes to validate your identity and tax return. In some cases, we may contact you for additional information. Also, the software product you use to E-file your taxes may ask for additional information. Our verification processes can take extra time and may delay your refund; however, they’re necessary to ensure the safety of your confidential information.

2015 MeF Individual/Business Test
Please only one product per sheet

Developer Name: _____ ETIN#: _____

Product Name: _____ NACTP#: _____

Individual or Business Tests: _____ Amended Return (Yes or No): _____

State only (Yes or No): _____

Contact Information

Primary Contact Name for MeF Individual/Business Tests: _____

Email Address: _____ Telephone: _____

Fax: _____

Secondary Contact Name for MeF Individual/Business Tests: _____

Email Address: _____ Telephone: _____

Fax: _____

Please Email : MeFtesting@tax.idaho.gov

2015 MeF Individual/Business Tests

Please select the Schemas and PDF attachments you will be submitting for testing

Schemas	Support	Schemas	Support	Schemas	Support
39R		55		75 Before June 30	
39NR		56		75 After July 1	
40		65		ID K-1	
41		66		PTE-01	
41S		67		PTE-12	
42		68		ITC-LIST	
43		68R			
44		69			
49		71			
49C		71R			
49R		CG			

Individual/Business Attachments

PDF Attachment	Attachment Name	Support
14	Form_14_01	
41A	Form_41A_01	
49E	Form_49E_01	
49ER	Form_49ER_01	
49ESR	Form_49ESR_01	
70	Form_70_01	
75-IC	Form_75IC_01	
75IMV	Form_75IMV_01	
402	Form_402_01	
NON-Idaho Income Tax Return	OtherState_Return_01	
Miscellaneous Statements	Misc_Stmt_01	
Combined Report Spreadsheet	Comb_Report_01	
ITC Equipment List	ITC_Equipment_01	
Reimbursement Incentive Credit	Reimburse_Credit_01	