MANUAL TRANSMITTAL

10.10.3

Department of the Treasury
Internal Revenue Service

AUGUST 18, 2023

EFFECTIVE DATE

(08-18-2023)

PURPOSE

(1) This transmits new IRM 10.10.3, Centralized Authentication Policy – Centralizing Identity Proofing for Authentication Across All IRS Channels.

(2) This transmits phase one of the new IRM 10.10.3 for the centralization of all authentication policy, where practical, and only includes current standard procedures, without change, used across most taxpayer facing Business Operating Divisions (BODs). Future updates will be made in collaboration with BOD IRM owners and subject matter experts for specialized procedures, gaps in policies, and where IRS modernization efforts require new or modifications to processes and procedures.

MATERIAL CHANGES

(1) None

EFFECT ON OTHER DOCUMENTS

None

AUDIENCE

The intended audience is IRS employees in areas who are in contact with taxpayers by correspondence, telephone/voice, in-person, remote in-person (video teleconferencing), and taxpayer digital communications, with the exception of employees in SB/SE Campus Examination/AUR Operations, and Field Operations whose current IRMs are not listed in the crosswalk as those procedures will be incorporated in a later revision of the IRM. Generally, if an IRM is in the related resource section and was used for identity proofing / identity verification, this IRM is now the official source of reference for authentication.

Angela R. Gartland
Director, Identity Assurance

10.10.3
Centralized Authentication Policy – Centralizing Identity Proofing for Authentication Across All IRS Channels

Table of Contents

10.10.3.1
(08-18-2023)
Program Scope and Objectives

(1) **Purpose:**This policy applies Centralized Authentication Policy concepts to IRS identity verification and authentication processes as a baseline for a taxpayer gaining access to tax account information.
This IRM is the official source for frontline employees working in taxpayer facing business units for performance of daily duties. Interim guidance procedures may be used to provide updates to the current procedures outlined in this IRM. Employees responding to taxpayer inquiries or other internal adjustment requests via any customer contact channel will use this IRM as a primary source. Not all procedures will be included in the first iteration of this IRM. The "basic", "enterprise", or routine procedures will be consolidated in the first iteration.
This IRM covers the policy and procedures from the Centralized Authentication Policy and consolidates identity verification and authentication policy across service channels into a single source of reference. This IRM provides procedures to assist frontline employees to answer correspondence, telephone, in-person, remote in-person (video teleconferencing), or online inquiries accurately and quickly and addresses gaps in pre-existing policy. This IRM:

a. Defines the uniform guidance, policies, and procedures to be followed by internal stakeholders.
b. Is based on the Omni-Channel best practices used across all IRS customer service applications, which is a recommendation in the IRS Authentication, Authorization, Access (A3) FY2022 Organizational Maturity Report and the 2020 Identity Assurance (Authentication) Strategy. The report and strategy were used as a basis for the consolidation of the authentication policies.
c. Creates a central reference source over time for identity proofing and authentication procedures streamlining the ability to update policy.
d. Ensures consistent integrated identity proofing and authentication procedures while incorporating emerging technology and security measures aiming to standardize procedures and reduce burden on business units.
e. Includes existing IRS authentication processes, developed procedures and solutions for reporting and security, and opportunities to improve user experience, where users go through the same identity proofing (or similar) across all IRS service channels.

(2) **Audience:** IRS employees who are in contact with taxpayers through correspondence, telephone/voice, in-person, remote in-person (video teleconferencing), and online exchanges (i.e., Wage & Investment, Small Business/Self Employed, Large Business & International, Taxpayer Advocate Service, Appeals, etc.).

(3) **Policy Owner:** Identity Assurance (IA), under Privacy Governmental Liaison and Disclosure, (PGLD) is the program office responsible for oversight, policy, and procedures for identity verification and authentication.

(4) **Program Owner:** The Director, IA reports to the Chief Privacy Officer and is responsible for IA program oversight.

(5) **Primary Stakeholders:** Management officials and employees within organizations and business units who authenticate taxpayers or representatives over digital and non-digital channels (correspondence, telephone/voice, in-person, remote in-person (video teleconferencing), and online exchanges).

(6) **Program Goals:** Provide authentication guidance for Accounts Management, Compliance, and every IRS employee who has the responsibility to authenticate the taxpayer to gain access to tax account information, as well as provide specific guidance on a variety of topics that may arise during taxpayer contacts.

10.10.3.1.1
(08-18-2023)
Background

(1) IRS employees must always verify the taxpayer's identity per IRM 13.1.16.4.1.1, Authorized Disclosures, before discussing any information protected under IRC 6103.

(2) This policy applies to the centralization of the identity proofing and authentication processes in customer contact channels (correspondence, telephone/voice, in-person, remote in-person (video teleconferencing), and online exchanges) where sensitive information is exchanged with individuals.
Non-digital channels: correspondence, telephone, in-person/remote in-person assistance.
Digital channels: online services/applications including website and mobile applications.

10.10.3.1.2
(08-18-2023)
Authority

(1) Relevant Federal guidelines include:

a. National Institute of Standards and Technology (NIST) Digital Identity Guidelines SP 800-63
b. U.S. Code (USC) 6103 Confidentiality and disclosure of returns and return information
c. Federal Information Security Modernization Act (FISMA)
d. Privacy Act of 1974
e. Office of Management and Budget (OMB) Memoranda M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management

10.10.3.1.3
(08-18-2023)
Responsibilities

(1) The Director of Identity Assurance (IA), within Privacy Governmental Liaison and Disclosure, (PGLD), is responsible for the identity verification and authentication policy.
The Director of IA reports to the Chief Privacy Officer and is responsible for IA program oversight.
Organization Executives and Management Officials who lead programs described in this policy are responsible for these guidelines and for continuous monitoring of new and ongoing authentication policies related to these channels.
IA's role is to strengthen and implement IRS authentication standards for:

- identity proofing,
- authentication,
- authorization, and
- access strategies, processes, and capabilities.

One component of the IA mission is to establish and maintain a Servicewide strategy that provides a framework for the Centralized Authentication Policy to consolidate policy with regard to identity proofing and authentication. This enables emerging technology and security measures to be incorporated into a single source of reference when those tools become available. The IRS will actively help taxpayers who try to follow the law, and work to continually improve the quality of systems and services to meet the needs of customers.

All taxpayers, whether delinquent or fully compliant, are entitled to prompt and professional service whenever they deal with Service employees. The public as a whole is the customer, not just delinquent taxpayers. Customers expect the IRS to promote voluntary compliance by ensuring that all taxpayers promptly pay their fair share.

10.10.3.1.4
(08-18-2023)
Program Controls

(1) Business Units are responsible for completing their own review. Management officials bear the responsibility to conduct risk assessments, of factors, procedures, and processes used to authenticate taxpayers, representatives or other third-parties interacting with the IRS. See Form 15295 , Non-Digital Authentication Risk Assessment (NDARA). The Identity Assurance function manages and reviews the Authentication in Digital and Non-Digital Channels Program at least once every two years. For more information regarding NDARAs, please refer to IRM 10.10.2, Authentication Risk Assessments in Non-Digital Channels. Goals, measures and operating guidelines are listed in each business unit's yearly Program Letter or other management guidance. Quality data and guidelines for measurement are referenced in IRM 21.10.1, Embedded Quality (EQ) Program for Accounts Management, Campus Compliance, Field Assistance, Tax Exempt/Government Entities, Return Integrity and Compliance Services (RICS), and Electronic Products and Services Support.

10.10.3.1.5
(08-18-2023)
Terms

(1) The below table lists commonly used terms and definitions relevant to this program that are used throughout this IRM:

Term	Definition
Access	The process of allowing an authenticated user to execute transactions or get to the data authorized by the taxpayer as provided through the authorization process. Access allows individuals to exercise the rights or privileges defined during authorization, based on successful authentication.
Authentication	The process of establishing or confirming that someone is the previously identified person they claim to be.
Authenticator Assurance Level (AAL)	The guidance on the selection, use, and management of authenticators (formerly called tokens) to authenticate a remote subscriber to an identity system.

Term	Definition
Authorization	The process that establishes the rights or privileges of users to interact with the IRS on behalf of themselves or others (e.g., businesses, individuals). Allows those users to exercise rights that have previously been established. Authorization is required for any person or business conducting IRS business on another person's behalf (such as a tax return preparer).
Channel	The means by which IRS interacts with external stakeholders.
Correspondence (mail, fax)	Communications through mail and fax.
Digital	Using or storing data or information in the form of digital signals. Involving or relating to the use of computer technology.
Disclosure	Making known the return or return information to any person in any manner
Identity Assurance (IA)	A function within Privacy, Governmental Liaison and Disclosure that supplies oversight and strategic direction for authentication, authorization, and access to enable the delivery of externally facing IRS services across all channels while protecting taxpayer data from fraudsters and identity thieves.
Identity Assurance Level (IAL)	The confidence level of the identity proofing process.
Identity Proofing	The process of establishing that a user is who they say they are.
Identity Verification	An authentication process that compares the identity a person claims to possess with data that proves it. There are many documents that can serve as proof: birth certificates, social security cards, driver's licenses, and others.

Term	Definition
In-Person/Remote In-Person	The channel in which in-person authentication is completed. For example, a taxpayer requesting a transcript may visit an IRS site or through video conferencing, to provide in-person/remote in-person identity proofing or authentication with an identification document, such as a driver's license.
Level of Assurance (LOA)	The degree of confidence that an individual is who they say they are for online transactions based on NIST 800-63-2, Authentication Guidelines.
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, Digital Identity Guidelines	Standards for federal agencies for implementing digital identity services. The guidelines cover identity proofing and authentication of users interacting with government IT systems over open networks as well as registration, authenticators, management processes, authentication protocols, federation, and related assertions.
Non-Digital	Not using the internet or computers, not represented by numbers; not digitized.
Telephone / Voice	Enterprise Architecture approved telephone and voice channels for external communications.

10.10.3.1.6
(08-18-2023)
Acronyms

(1) The following table lists acronyms and definitions frequently used throughout this IRM section:

Acronym	Definition
A3	Authentication, Authorization and Access
AAL	Authenticator Assurance Level
ACS	Automated Collection System
AMS	Account Management Services
AOR	Address of Record

Acronym	Definition
BMF	Business Master File
CAF	Centralized Authorization File
CC	Command Code
DBA	″Doing Business As″
DOB	Date of Birth
EFIN	Electronic Filer Identification Number
EHSS	E-help Support System
EIN	Employer Identification Number
EQ	Embedded Quality
FAL	Federal Assurance Level
HRA	High Risk Authentication
IA	Identity Assurance
IAL	Identity Assurance Level
IDRS	Integrated Data Retrieval System
IM	Incident Management
IMDs	Internal Management Documents
IMF	Individual Master File
IP PIN	Identity Protection Personal Identification Number
IRSN	Internal Revenue Service Numbers
ITIN	Individual Taxpayer Identification Number
IVR	Interactive Voice Response
LOA	Level of Assurance
MOD IEIN	Modernized Internet Employer Identification Number
NIST	National Institute of Standards and Technology
OPA	Online Payment Agreement
ODC	Oral Disclosure Consent
PGLD	Privacy, Governmental Liaison and Disclosure
PII	Personally Identifiable Information
POA	Power of Attorney
PPKM	Privacy Policy and Knowledge Management
PTIN	Preparer Tax Identification Number
QSR	Quality Site Requirement
RICS	Return Integrity and Compliance Services

Acronym	Definition
RTS	Real-Time System
SBU	Sensitive But Unclassified
SSN	Social Security Number
TAC	Taxpayer Assistance Center
TCE	Tax Counseling for the Elderly
TIA	Tax Information Authorization
TIN	Taxpayer Identification Number
TPP	Taxpayer Protection Program
VITA	Volunteer Income Tax Assistance
VSD	Virtual Service Delivery

10.10.3.1.7
(08-18-2023)
Related Resources

(1) Below are the related resources:

- Privacy Act of 1974 (as amended),
- IRC 6103, Confidentiality and Disclosure of Returns and Return Information,
- NIST SP 800-63-A guidelines,
- IRM 10.5.1, Privacy and Information Protection, Privacy Policy,
- IRM 10.5.4, Privacy and Information Protection, Incident Management Program,
- IRM 10.5.5, Privacy and Information Protection, Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements, and
- IRM 11.3.1, Disclosure of Official Information, Introduction to Disclosure.

(2) In the event an inadvertent disclosure occurs or an unauthorized access takes place, see the following IRMs for guidance, IRM 10.5.1, Privacy and Information Protection, Privacy Policy, IRM 10.5.4, Privacy and Information Protection, Incident Management Program, IRM 10.5.5, Privacy and Information Protection, Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements, and IRM 11.3.1, Disclosure of Official Information, Introduction to Disclosure.
The following table lists the primary sources of guidance:

Previous IRM that Housed the Authentication Policy	Previous IRM Title that Housed the Authentication Policy	Channel
IRM 3.21.263.7.1.1	TAC Disclosure Guidelines for ITIN Data	In-Person
IRM 3.21.263.8.1	Disclosure Guidelines for ITIN Data	Phone

Previous IRM that Housed the Authentication Policy	Previous IRM Title that Housed the Authentication Policy	Channel
IRM 3.21.264.3.3	Disclosure Guidelines for Acceptance Agents	Phone
IRM 5.19.1.2.3.2	Additional Taxpayer Authentication	Phone
IRM 5.19.1.2.3.3.1	Transfer Personal Identification Number (PIN) Acceptance	Phone
IRM 8.6.5.2	Identity Theft General Documentation Requirements	Correspondence
IRM 21.1.1.4	Communication Skills/ Outgoing Calls	Phone
IRM 21.1.3.2.3	Required Taxpayer Authentication	Phone
IRM 21.1.3.2.4	Additional Taxpayer Authentication	Phone
IRM 21.1.3.3	Third-Party (POA/TIA/F706) Authentication	Phone
IRM 21.1.3.3.1	Third-Party Designee Authentication	Phone
IRM 21.1.3.3.2	Oral Disclosure Consent/ Oral TIA (Paperless F8821)	Phone
IRM 21.2.1.57	Online Payment Agreement (OPA) for IMF Debts	Online
IRM 21.2.1.57.1.1	Verification Issues for BMF OPA Users	Online
IRM 21.2.1.58.1	Secure Access eAuthentication	Online
IRM 21.2.3.3.3	Interactive Voice Response	Phone
IRM 21.3.4.2.3	Virtual Service Delivery (VSD)	In-Person/ Remote In-Person
IRM 21.3.4.26.1	Letter 5881-C or 5877-C Contacts	In-Person
IRM 21.3.8.4.1.5	Issue and Entity Identification and Taxpayer Authentication Procedures	Phone
IRM 21.3.8.5.1.3.3	Status of Pending (Open) Employee Plans (EP) Determination/Application Requests	Phone

Previous IRM that Housed the Authentication Policy	Previous IRM Title that Housed the Authentication Policy	Channel
IRM 21.7.1.4.7.1	Employer Identification Number (EIN) Verification and Requests for Letter 147C, EIN Previously Assigned	Phone
IRM 21.7.13.3.4.1	Modernized Internet EIN (Mod IEIN)	Phone
IRM 21.7.13.3.9.1	Form SS-4 Application Status	Phone
IRM 22.30.1.8.1.1.3	Preparing Returns Using Virtual VITA/TCE	In-Person
IRM 22.30.1.8.9.4.1.1	Individual Taxpayer Identification Number/ Social Security Number "ITIN/SSN Mismatch"	In-Person
IRM 22.30.1.8.12.1	Quality Site Requirements (QSR)	In-Person

10.10.3.2
(08-18-2023)
Understanding Identity Proofing for Authentication

(1) Various business units authenticate taxpayers, representatives, or other third-parties through a form of identity proofing or identity verification. This is done to ensure the taxpayer or customer is who they say they are and to keep unauthorized individuals from accessing taxpayer/customer data they are not entitled to receive. The following subsections cover procedures that are handled through a variety of IRS channels. These channels include correspondence, telephone/voice, in-person, remote in-person (video teleconferencing), and online exchanges. The procedures consolidated in this IRM have been broken down into subsections by channel.

10.10.3.3
(08-18-2023)
Telephone/ Voice

(1) Frontline employees engage in external communications via telephone and voice channels. Procedures for telephone and voice channels are contained in the following sections.

(2) Prior to providing authorized tax return information, ask for identifying information and conduct IDRS research to validate the responses (e.g., name and TIN). For a list of the research command codes, refer to IRM 21.1.3.2.3(10), Required Taxpayer Authentication, for additional information

10.10.3.3.1
(08-18-2023)
Identity Proofing for Disclosure Guidelines for ITIN Data

(1) This subsection of the IRM provides guidance and procedures for IRS employees in Austin Submission Processing Campus ITIN Operations, Accounts Management Customer Service Representatives, and Field Assistance. The following identity proofing process will be used when securing information from the caller to verify the applicant in question and to compare it

to the information on the Real Time System (RTS), W-7 Application View screen during the ITIN disclosure process.

Note: If the caller provides the ITIN they are inquiring about, you can use the number to locate the application in RTS then proceed with the disclosure guidelines.

- Name – Line 1a
- Name at Birth – Line 1b, if different from Line 1a
- Date of Birth – Line 4
- Country of Birth – Line 4
- Country of Citizenship – Line 6
- Previously Issued ITIN or IRSN – Lines 6e and 6f
- Types of supporting ID submitted

Caution: If unable to verify the required fields, verify two or more additional entries from the application (for example, country issuing documentation, date of entry, or educational institution/company name/city).

(2) You must also verify the relationship of the caller to the applicant before disclosing any information. The following signature relationships are reflected on RTS:

- Applicant
- Parent
- Court Appointed Guardian
- Power of Attorney
- None

(3) The RTS captures the relationship of the person who signed the Form W-7 as well as the name if other than the applicant. The table below provides additional guidance for signature verification.

If...	**Then...**
Parent box is checked in the signature area,	The parents name is in the ″Name of delegate″ field. Compare this to the information provided by the caller.
Power of Attorney box is checked in the signature area,	Form 2848 was submitted with Form W-7, and the representatives name is in the ″Name of delegate″ field. Compare this to the information provided by the caller.
Court-appointed box is checked or Legal guardian is shown in the signature area,	Court document granting guardianship was submitted with Form W-7 provided, and the guardians name is in the ″Name of delegate″ field. Compare this to the information provided by the caller

If...	Then...
Third-party inquires about the status of an ITIN application and is **not** listed as parent, POA, court appointed guardian, or Acceptance Agent on original application.	If in Assigned Status, advise information will be sent to the address of record. For any other status, advise information can only be shared with the authorized person of record. If caller states a Form 2848 or court document was attached to application, but the application shows no record of a POA or court document take the following actions: ***Caution:*** If a Form 2848 was submitted after the original Form W-7 was processed, the POA name is recorded in the Remarks Screen. • If in Suspense (S 14) Status, advise the caller to resubmit the documents to the Austin ITIN Unit • For any other status, see IRM 21.1.3.3, Third-Party (POA/TIA/F706) Authentication, if no Form 2848 is found. See IRM 21.1.3.3.2 Oral Disclosure Consent/ Oral TIA (Paperless F8821), for Oral Disclosure Consent. • If the caller has a tax related (non-ITIN) issue, follow normal AM procedures for handling calls • If the conversation reveals that the authorized person will be calling from abroad, the CSR should provide the International Accounts Management telephone number (267) 941-1000 and inform them that it is not a toll-free number.

(4) If a caller indicates that they are a Certifying Acceptance Agent(CAA), and is inquiring about the status of an application, refer them to their signed CAA agreement and have them call the number listed in the agreement.

10.10.3.3.2
(08-18-2023)
Identity Proofing for Disclosure Guidelines for Acceptance Agents

(1) This subsection of the IRM provides guidance and procedures for the IRS Acceptance Agent (AA) Program. Use the following table to authenticate a customer and their authority to receive information about an Acceptance Agent application:

Position/Relationship	Authentication Requirements
Principal, Partner, or Owner	EIN, legal or DBA name, physical or mailing address
Authorized Representative (U.S. Citizen)	SSN, name, address, filing status as shown on last return, and DOB
Authorized Representative (non-resident alien)	PTIN, name, address, DOB
Authorized Representative (foreign national)	PTIN, name, address, DOB (CC RPVUE for foreign nationals)
Primary or Alternate Contact	EIN, title, phone number, e-mail address

Note: If the required disclosure information for an Authorized Representative is not available in the Real Time System (RTS), search E-help Support System (EHSS) with the EIN. If the application is found, authenticate the caller by asking for the EIN, company name, EFIN (if applicable), and what date they sent the application. Tell the customer that the application is in inventory only; do not provide the application place in inventory or speculate when the application will be completed. If you cannot authenticate the caller from information in EHSS, escalate the case to Austin Leads Provider group and provide customer name, company name (legal or DBA) role, EIN, telephone number with time zone and hours of availability, EFIN (if available) or business address. Provide the Incident Management (IM) to the customer and tell them they will receive a call back.

10.10.3.3.3
(08-18-2023)
Identity Proofing for Additional Taxpayer Authentication for Collection Employees

(1) This subsection of the IRM provides guidance and procedures for:

- ACS and ACSS employees,
- CSCO employees, and
- FA employees.

The *IAT Disclosure Tool* assists in verifying the identity of a caller and determining if the caller is authorized to receive confidential tax information. When responding to balance due inquiries, Collection employees will use the *IAT Disclosure Tool's* tool to assist them in verifying the identity of a caller and determining if the caller is authorized to receive confidential tax information or represent the taxpayer. There will be times when systemic issues may cause problems with the IAT Disclosure tool's performance. When this occurs, ask the taxpayer to provide two or more of the following items and perform manual research to verify the caller's responses:
Use the following table to determine which authentication probes to use for IMF Accounts:

Additional Authentication Probes: IMF Accounts
Filing status on return in question
Spouse's date of birth
Childs'/children's date(s) of birth
Amount of income reported on last return or tax due on return
Employers shown on taxpayer's Form W-2
Financial institutions from taxpayer's Form 1099-INT or Form 1099-DIV
Number of exemptions claimed on last return or on return in question
Preparer, paid/unpaid, if any
Expected refund amount (within $100) **unless** computed by IRS
Any other verifiable items from the return/account

Note: When considering what probes to ask, determine which probes would most likely be known by an authorized party. Try to eliminate those that may be easily discoverable or guessed

Use the following table to determine which authentication probes to use for BMF Accounts:

Additional Authentication Probes: BMF Accounts
Federal income tax withheld/Social Security wages Form 941
Gross receipts or sales/Taxable income Form 1120
Total assets/Total liabilities Form 990
Any other verifiable items from the return/account

Note: When considering what probes to ask, determine which probes would most likely be known by an authorized party. Try to eliminate those that may be easily discoverable or guessed

10.10.3.3.4
(08-18-2023)
Identity Proofing for Transfer Personal Identification Number (PIN) Acceptance

(1) This subsection of the IRM provides guidance and procedures for:

- ACS and ACSS employees,
- CSCO employees, and
- FA employees.

Taxpayers may inform an IRS assistor they have a four (4) digit transfer PIN provided by the previous IRS assistor. When this occurs, ACS assistors must ask for the following:

- Taxpayer's Name and TIN,
- Transfer PIN,

- Caller's Name, and
- Purpose of the call.

Caution: The Transfer PIN may only be used by taxpayers. If a third party attempts to use a Transfer PIN, **do not** accept it. Instead see IRM 5.19.1.2.3.3.1, Transfer Personal Identification Number (PIN) Acceptance, para 5.

10.10.3.3.5
(08-18-2023)
Identity Proofing for Communication Skills/Outgoing Calls

(1) This subsection of the IRM provides guidance and procedures for Wage and Investment (W&I) and Small Business/Self Employed (SB/SE) Business Operating Divisions (BODs) handle taxpayer contacts when

a. Providing general tax related information,
b. Providing information on the status of taxpayer returns/refunds/accounts, and
c. Adjusting taxpayer accounts, when proper.

The following identity proofing process will be used when verifying the requestor's identity for when you initiate an outgoing phone call, the taxpayer may be reluctant to give you his/her TIN:

a. Provide the taxpayer with the last four digits of their TIN (Social Security Number/Employer Identification Number).
b. Request that the taxpayer verify the first five digits of their TIN.
c. After verifying the TIN, follow IRM 21.1.3.2.3, Required Taxpayer Authentication and IRM 10.10.3.6, Identity Proofing for Required Taxpayer Authentication.

10.10.3.3.6
(08-18-2023)
Identity Proofing for Required Taxpayer Authentication

(1) This subsection of the IRM provides guidance and procedures for All IRS employees, in Business Operating Divisions (BODs), who are in contact with taxpayers by telephone, correspondence, or in person. The primary users of this IRM are all employees within LB&I, SB/SE, TE/GE, TAS and W&I. Use the following identity proofing process to verify the requestor's identity for Required IMF Authentication Probes. Request and validate the correctness of:

- Taxpayer Identification Number (TIN) – Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN) – If the taxpayer is inquiring about a jointly filed return, only one TIN is necessary, preferably the primary number. The secondary TIN may be required if the primary is unavailable, or for use as an additional authentication check. See IRM 3.21.263.8.1, Disclosure Guidelines for ITIN Data, for specific ITIN research and IRM 10.10.3.4.1, Identity Verification for Disclosure Guidelines for ITIN Data.

  Note: In the event the name and TIN provided by the caller at the beginning of the call do not match our records, ask the caller to verify their information. After probing, if the information provided still does not match our records, ask the caller to check their records and call back. Terminate the call.

- Name – as it appears on the tax return (for the tax year(s) in question), including spouse's name for joint return.

  Caution: Do not confirm or deny any information until authentication is complete. The decision to authenticate is made at the conclusion of all the necessary probes along with additional authentication when needed to help make that determination.

If the caller is inquiring about multiple tax periods and MFTs you must be certain that the individual is authorized to receive information on each tax period and MFT.

- Current address – If taxpayer fails to provide the correct address of record, but correctly responds to all of the other items, (IMF – name, TIN and date of birth) you may request additional taxpayer authentication pursuant to IRM 10.10.3.3.7, Identity Proofing for Additional Taxpayer Authentication.

  Note: If you are unable to verify the address on the Integrated Data Retrieval System (IDRS), request the address as it appears on the last tax return or as modified by IRS records.

- Date of birth (DOB) of primary or secondary taxpayer – If the taxpayer fails the DOB probe, but correctly responds to all other items above (IMF – name, TIN, and address), you may request additional taxpayer authentication pursuant to IRM 10.10.3.3.7, Identity Proofing for Additional Taxpayer Authentication.

  Note: If there is a discrepancy with the DOB in IRS records on IDRS (CC INOLE) for an SSN but you are confident (i.e., taxpayer has passed authentication requirements) that you are speaking with the taxpayer, advise the taxpayer to contact the Social Security Administration (SSA) at 800-772-1213 or www.ssa.gov to correct the error. For DOB discrepancies on an ITIN, refer to IRM 3.21.263.8, Accounts Management (AM).

  Caution: Filing status was removed as a required probe on December 12, 2011; however, knowledge of the filing status of any year or multiple years in question is vital to understanding if the individual inquiring is entitled to receive information on a given tax year. Take caution on any jointly filed return to ensure the individual is authorized to receive the information on the year or years in question.

  Reminder: See Exhibit 21.2.2-2, Accounts Management Mandated IAT Tools for those employees mandated to use *IAT Disclosure Tool*.

(2) For first time filers, if the return is not completely processed or rejected, you can verify:

- Amount of refund and filing status on CC FFINQ
- Name Control and DOB on CC INOLES
- Complete Name and DOB on CC DDBKD

(3) For Required BMF Authentication probes, the following information should be requested:

a. Taxpayer Identification Number, Employer Identification Number or Social Security Number.

Note: If the customer is unable to provide the TIN but correctly responds to the name probe, request additional authentication. See IRM 10.10.3.3.7, Identity Proofing for Additional Taxpayer Authentication.

For example, a previously issued EIN that has not been recently used or an EIN that was recently assigned.

b. Name – as it appears on the account or as shown on CC INOLES. It may be necessary to probe the caller for the correct information using additional authentication information such as Limited Liability Company (LLC) or ″Doing Business As″ (DBA) for Sole Proprietor/Partnership. A member's LLC authority is determined by the type of business entity and the member's authority within that business structure. See IRM 11.3.2.4, Persons Who May Have Access to Returns and Return Information Pursuant to IRC Section 6103(e), for more detailed information on who can have access to types of business entities.

Caution: Do not confirm or deny any information until authentication is complete. The decision to authenticate is made at the conclusion of all the necessary probes along with additional authentication when needed to help make that determination. If the caller is inquiring about multiple tax periods and MFTs you must be certain that the individual is authorized to receive information on each tax period and MFT.

c. Current address – If taxpayer fails to provide the correct address of record, but correctly responds to all of the other items (e.g., Name and Title) request additional taxpayer authentication pursuant to IRM 10.10.3.3.7, Identity Proofing for Additional Taxpayer Authentication.

Note: If you are unable to verify the address on IDRS, request the address as it appears on the last tax return or as modified by IRS records.

d. For Form 709(MFT 51) calls, the disclosure probes are TIN, name and address of the return and date of birth of the taxpayer.

e. For Form 706(MFT 52) calls, the disclosure probes are SSN of the estate, name and address on the return and date of death or date of birth of the taxpayer, whichever is applicable.

Reminder: If available, you may use AMS Privacy and Disclosure screens to access IDRS.

10.10.3.3.7
(08-18-2023)
Identity Proofing for Additional Taxpayer Authentication

(1) This subsection of the IRM provides guidance and procedures for All IRS employees, in Business Operating Divisions (BODs), who are in contact with taxpayers by telephone, correspondence, or in person. The primary users of this IRM are all employees within LB&I, SB/SE, TE/GE, TAS and W&I. The following identity proofing process will be followed when Accounts Management employees are conducting additional taxpayer authentication. If conditions require for additional taxpayer authentication, the use of the IAT Disclosure Tool is mandated. If the tool is down, then manual authentication is required.

Note: Employees working the Taxpayer Protection Program (TPP) should follow authentication procedures in IRM 25.25.6.4, Taxpayer Protection Program (TPP) High-Risk Authentication (HRA) Procedures when the caller confirms they filed the return in question. Employees taking phone calls on the TPP application should choose the TPP HRA option on the IAT Disclosure Tool.

(2) After required authentication is completed, the IAT Disclosure Tool will allow you to choose any tax year. When possible, you should select the most recent year available to attempt additional high-risk authentication, or the most appropriate year depending on any specific account conditions or available tax documents. You may also select from a list of previous years, including a tax year where there is no processed return. If there is enough data present on

mandated for the Taxpayer Protection Line.

Note: The tool selects from command codes IRPTRL, RTVUE/BRTVU, TRDBV, INOLET, IMFOLT/BMFOLT and DDBKD. A list of questions for IMF asked by the tool can be found in IRM 25.25.6.4, Taxpayer Protection Program (TPP) High Risk Authentication (HRA) Procedures, under the **Possible Questions** column. You can use this list as a good source of questions when manual authentication research is necessary.

(3) If there is not enough data present in the year selected, the tool will provide an

current filings, then you may use the tool's manual authentication process. It will provide a drop-down menu of the available sources listed above and then you can choose a source to manually research, choosing questions that would

preferred but not required on manual research if the account data is limited. Some BMF entity types will have limited data and can be passed with at least two correct responses from one data source.

(4) For both IMF and BMF, the tool will provide a pass/fail response once you have asked all the questions presented and marked the appropriate response. The tool should provide the appropriate error message if any of the questions are not answered. Once verified, assist the caller following normal IRM procedures. Use AMS issue/narrative to leave a brief note recording any failed disclosure.

Note: It is important for the caller to answer all the questions presented by the tool. The tool recently added the command code VERIF. That command code will work in the background to collect data from responses to IMF questions. The data will be used to help shape future policy decisions on the disclosure process. VERIF does not collect data on the BMF side.

(5) There will be other situations when some manual research may be necessary. Calls on married filing joint accounts from the secondary SSN may require some manual research since data pulled from the primary on some command codes are unique to that SSN (e.g., city of birth).

(6) For calls where the taxpayer has an ITIN, you can attempt to use the enhanced HRA tool to generate questions and validate the caller. Some questions generated on the tool will require access to the ITIN RTS to validate the response.

(7) For some dependent questions pulled by the tool, there may be multiple responses in the answer portion such as the SSN and date of birth field. Consider the question a pass if the caller provides one correct SSN or DOB from those provided.

Note: The data source for dependent names will only provide those born after 1998.

(8) There will be times when systemic issues may cause problems with the tool's ability to produce the needed data to authenticate due to temporary command code outages or an IDRS issue. Manual research is required for both IMF and BMF accounts when the tool is unable to produce the necessary information to validate the caller. Use the data available from the account or return to attempt to validate at least two additional items from multiple data sources when possible.

(9) When considering what probes to ask on IMF or BMF, determine which probes would most likely be known only by an authorized party. Try to eliminate those that may be easily discovered or guessed.

Reminder: Testing and piloting will not uncover all potential issues on any tool. IAT will continue to work to resolve any issues that come up on the revised Disclosure Tool. Prior to opening a ticket on any issue please check the *IAT Known Issue Page* for any reported problems.

10.10.3.3.8
(08-18-2023)
Identity Proofing for Third-Party (Oral Disclosure Consent, (ODC)) Authentication

(1) This subsection of the IRM provides guidance and procedures for All IRS employees, in Business Operating Divisions (BODs), who are in contact with taxpayers by telephone, correspondence, or in person. The primary users of this IRM are all employees within LB&I, SB/SE, TE/GE, TAS and W&I. The following identity proofing process will be followed when authenticating the Oral Disclosure Consent Designee. You will need to know the form and period in question along with the following:

- Taxpayer's Name
- Taxpayer's TIN
- Third-party Name
- Third-party Phone Number

10.10.3.3.9
(08-18-2023)
Identity Proofing for Third-Party Designee Authentication

(1) This subsection of the IRM provides guidance and procedures for All IRS employees, in Business Operating Divisions (BODs), who are in contact with taxpayers by telephone, correspondence, or in person. The primary users of this IRM are all employees within LB&I, SB/SE, TE/GE, TAS and W&I. To authenticate the caller as a Third-Party Designee, research CC TXMOD (IMF and BMF), CC IMFOL, CC BMFOL, CC RTVUE, CC BRTVU, CC TRDBV or CC ERINVC and follow the identity proofing procedure below by asking for:

- Taxpayer's Name – as it appears on the tax return for the tax year(s) in question, including spouse's name for a joint return
- Taxpayer's TIN
- Tax Period
- Form(s)
- Designee's PIN or Designee's PTIN – PTIN option is for BMF only, on any forms that still contain the Third-Party Designee check box in the Paid Preparer Use Only field

Note: If there is a TC 971 AC 263 on the account, do not use CC TRDBV, CC RTVUE or CC BRTVUE, as it is not updated to reflect revocation.

(2) Validate the identification number provided by the Third-Party Designee with the posted data using the following identity proofing procedure below:

- Self-selected PIN – research using CC TXMOD
- PTIN (for certain applicable BMF forms) – validate the PTIN information provided by the designee with the data on CC TXMOD, CC IMFOLR, CC BMFOLR, CC RTVUE or CC BRTVU to ensure they match.

(3) BMF taxpayers may designate a Third-Party Designee on any BMF return. All BMF returns contain either a Third-Party Designee Section or a Paid Preparer Designee check box. To authenticate the caller as the Third-Party Designee, research IDRS for the presence of the check box field (see IRM 10.10.3.9, Identity Proofing for Third-Party Designee Authentication, follow the procedures above in paragraph 1 in this section. The following information is entered in the Third-Party Designee section:

- Designee Name
- Designee Phone Number
- Any five-digit number the Designee chooses as their Personal Identification Number (PIN).

Note: The authority granted on a BMF return using the check box option also extends to any amended return filed for the year in question, as long as it is filed within the time period for the consent.

10.10.3.3.10
(08-18-2023)
Identity Proofing for Oral Disclosure Consent/Oral TIA (Paperless F8821)

(1) This subsection of the IRM provides guidance and procedures for All IRS employees, in Business Operating Divisions (BODs), who are in contact with taxpayers by telephone, correspondence, or in person. The primary users of this IRM are all employees within LB&I, SB/SE, TE/GE, TAS and W&I. The following identity proofing process will be used when the IRS is obtaining a taxpayer's non-written consent to disclose:

a. Gather sufficient facts underlying the request or consent to enable the employee to determine the nature and extent of the information or assistance requested and the return or return information to be disclosed.
b. Confirm the identity of the taxpayer and the designee.
c. Confirm the date requested and the nature and extent of the assistance request.

10.10.3.3.11
(08-18-2023)
Identity Proofing for Interactive Voice Response

(1) This subsection of the IRM provides guidance and procedures for AM assistors. Taxpayers must verify their identity to use the Interactive Voice Response (IVR) to obtain Transcript Delivery System (TDS) tax return and tax account transcripts. Taxpayers are prompted to enter their:

- Social Security Number (SSN) or Individual Taxpayer Identification number (ITIN).
- Numbers/digits in the street address currently on file.

For more information on IVR, please refer to IRM 21.2.3.3.3, Interactive Voice Response.

10.10.3.3.12
(08-18-2023)
Identity Proofing for Issue and Entity Identification and Taxpayer Authentication Procedures

(1) The following identity proofing process will be used when the caller needs to authenticate an entity or taxpayer in order to ensure that both parties are talking about the same entity and to avoid the unauthorized disclosure of information protected under IRC 6103. These calls are received in Tax Exempt/ Government Entities (TEGE) Customer Account Services (CAS). Ask the caller for:

- name,
- address,
- and EIN of the organization/plan sponsor in question.

Compare the caller's response to the information in our records using the available research tools.

Note: For purposes of entity identification *(but **NOT** when establishing the caller's authority as noted in the Reminder that follows*), disregard minor discrepancies in the name or address of the entity (e.g., omission of ″INC″ from the organization's name, ″suite″ instead of ″apartment,″ ″street″ instead of ″avenue,″ or the omission of a building name) **as long as you are reasonably sure that you and the caller are referring to the same entity**. Do not treat the c/o name line as part of the address for purposes of entity identification.

Reminder: When attempting to determine the caller's authority to receive information protected under IRC 6103 or to perform certain actions such as making an address change over the telephone, it may be necessary to prompt the caller to provide the entity's exact name or address of record. If the caller is unable to do so, refer to the alternative disclosure prompts discussed in paragraph 11, IRM 21.3.8.4.1.5, Issue and Entity Identification and Taxpayer Authentication Procedures.

Caution: The names of subordinate organizations may appear on the primary name line or on the sort name line, depending on the nature of the group ruling. If the caller is inquiring about a subordinate organization and correctly identifies the name of the subordinate as it appears on the sort name line, it is not necessary for the caller to identify the exact name of the central organization as it appears on the primary name line as long as you are reasonably sure that the correct subordinate organization has been identified.

(2) If the caller is unable to provide all of the identifying information such as the city and/or state when the full address is not known, attempt to secure as many details as possible. If you are able to locate information open to public disclosure under IRC 6104, advise the caller that the information being provided is based on our available records.

Example: A caller asks about the exempt status of an organization for which they has only the name. Using CC NAMEE, you are able to locate organizations with that name in Maine, Ohio, Nebraska, and Virginia. Additional IDRS research shows that only the organizations in Nebraska and Virginia are exempt by virtue of an approved application, (i.e., the organizations have tax-exempt status under section 501(a) of the Internal Revenue Code). Disclose information to the caller about the organizations in Nebraska and Virginia but advise the caller that, because she was not able to provide complete identifying information, there is no

guarantee that either of the organizations that you located is actually the organization about which they called. Tell them that they may call again if they obtain additional identifying information that indicates that neither of the exempt organizations you located is the correct organization.

(3) There are limitations to the research you can perform when the caller cannot provide enough information:

- If you receive the message, ″XXXXX POSSIBLE MATCHES, SUPPLY ADDITIONAL INFO,″ when you perform your CC NAMEE/NAMEB research, apologize to the caller and explain that we are unable to perform adequate research with the limited information provided. Invite the caller to contact us again if they can provide additional identifying information about the organization.
- If your CC NAMEE/NAMEB research returns more than 15 – 20 pages of data (or if you receive the message, ″XXXXX MATCHES – DISPLAY LIMIT EXCEEDED,″ consult your Lead.

(4) NEVER offer sensitive information such as the name of the organization/plan sponsor/plan, c/o person name, current address, or other account-specific information to a caller when attempting to identify the entity or to confirm authorization. Instead, ask the caller to provide the information and then compare the response to the information on record. Offering information that is present on the Master File or EDS/TEDS record could compromise your ability to verify that the party is authorized, if necessary, and could result in an unauthorized disclosure.

Reminder: When disclosing information open to the general public under IRC 6104, you may provide the caller with any identifying information not known to the caller **as long as it is disclosable under IRC 6104**. If the caller is authorized but does not know the current address of record (AOR) and you disclose the AOR to that caller, oral statement procedures for updating the address will not apply. Form 8822-B (or Form 990-N, etc.) will be required for an address update.

(5) Once you have identified the organization/plan sponsor/plan, you must determine whether the information requested by the caller is open to inspection under IRC 6104 or is protected under IRC 6103 and open only to authorized individuals. Unless the information being requested is open to the general public under IRC 6104 or is available through IRS publications or on IRS Web pages, you must verify that the customer is an authorized party. This applies to all verbal and written disclosures.

Reminder: When performing disclosure verification, take all necessary steps to assure yourself that the caller is an authorized party and entitled to the information requested.

Caution: If the caller's question/issue changes from one covered by IRC 6104 to one covered by IRC 6103, you must determine the caller's authority to receive the information before disclosing it.

(6) If the information requested by the caller is protected under IRC 6103, you must determine the caller's relationship to the organization/plan sponsor/plan in

question. If the caller did not include that information with the opening or subsequent statements (for example, ″I am the president of our local PTA and I want to check on the status of our application for exemption″).

Note: Using a purpose statement (such as, ″In order to protect the organization and the IRS, I need to verify your relationship with the organization before disclosing certain information″) before asking the caller the disclosure prompts can help put the caller at ease and can make you feel more comfortable asking the disclosure prompts.

Reminder: Organizations can have varying titles for their officers. The key is to establish that the person with whom you are in contact is legally authorized to act on behalf of the organization and is not an outside third party. See IRM 21.3.8.4.3.1, Employee Plans Disclosure Explanation of Terms, for information specific to plan administrators.

Caution: When the caller's issue involves an employee plan, you must research the appropriate master file to determine the caller's authority. For example, account calls on Form 5500, Annual Return/Report of Employee Benefit Plan, or Form 5500-EZ, Annual Return of A One-Participant (Owners/Partners and Their Spouses) Retirement Plan or A Foreign Plan, (MFT 74) and on Form 8955-SSA Annual Registration Statement Identifying Separated Participants With Deferred Vested Benefits, (MFT 75) are to be verified via the Employee Plan Master File (EPMF) by inputting a ″P″ at the end of the plan sponsor's EIN. Account calls on Form 5330, Return of Excise Taxes Related to Employee Benefit Plans, (MFT 76) are to be verified via the Business Master File (BMF) by using the filer's identifying number (EIN or SSN with a ″V″ at the end). See IRM 21.3.8.4.1.5 paragraph (11), Issue and Entity Identification and Taxpayer Authentication Procedures, if the caller is attempting to demonstrate authority and is unable to give the correct address of record for the appropriate Master File account.

(7) If the caller is an officer, employee, or other designated person within the organization/plan sponsor, and is not an outside third party, verbal confirmation that the caller is authorized to act on behalf of the organization/plan sponsor/plan is sufficient verification for Exempt Organization and Employee Plan disclosure once the caller's position within the organization/plan sponsor is established (and the correct organization/plan has been identified).

Example: If the caller has stated they are the current treasurer of the organization, ask the caller if, as treasurer, they are legally authorized to act on behalf of the organization.

Note: Identifying the plan by name, although necessary before providing information specific to the plan, is not part of the authentication process for officers of the plan sponsor, but it is part of the authentication process when establishing the authority of third parties.

- If the caller represents a government entity, see IRM 21.3.8.4.4.2, Instrumentality/Governmental Units Disclosure, for additional information.

- If the caller is a plan participant seeking information pertaining to a plan, see IRM 21.3.8.4.1.5.1, Authorization Requirements for Participants in an Employer-Sponsored Plan.
- See IRM 21.3.8.5.1.3.2, Status of Pending (Open) Exempt Organization (EO) Determination/Application Requests, , if the caller is checking on the status of a pending (open) application and does not have the organization's EIN.

Caution: A trustee may be an outside third party who is not authorized without specific authority.

Reminder: Certain issues and categories of callers require additional research:

- See IRM 21.3.8.5.1.3.3, Status of Pending (open) Employee Plans (EP) Determination/Application Requests, if the caller is checking on the status of an EP application.

(8) If the caller being screened for authorization cannot provide the entity's exact name, correct address of record, or the caller's position with the organization/plan sponsor does not clearly identify the caller as an officer (but the caller correctly responds to the other disclosure prompts), additional probing is necessary to help establish that the party is authorized. Ask the caller at least two organization-specific questions about any information found on the master file record (such as specific return information or EO information), or information found on EDS/TEDS, for example:

- The date the organization's application for recognition of exemption was filed
- The amount of user fee paid with the application for recognition of exemption
- Specific line items from filed returns

Caution: These high risk authentication procedures apply only to callers authorized by their position in the organization, not to third parties.

(9) If the caller is unauthorized, apologize and explain that disclosure laws prevent you from being able to respond to the question and provide general guidance or information open under IRC 6104 to the extent that is possible. Tell the caller that an officer legally authorized to act on behalf of the entity can call anytime for the requested information.

(10) Before an outside third party (e.g., an accountant, bookkeeper, or attorney) can be considered as authorized to receive information protected under IRC 6103, disclosure rules require:

- Formal execution of authorization (i.e., Form 8821 / Form 2848)
- Oral Consent by an authorized party (for specific account matters) **or**
- Specification of a Third-Party Designee on the return

10.10.3.3.13
(08-18-2023)
Identity Proofing for Status of Pending (Open) Employee Plans (EP) Determination/Application Requests

(1) This subsections of the IRM provides guidance for Customer Service Representatives (CSRs) and Customer Service Specialists (CSSs) in responding to telephone inquiries from Tax Exempt/Government Entities (TEGE) customers. The following identity proofing process will be used when the caller wants to know the status of a pending (open) EP determination/application request:

a. Obtain the name and address of the plan sponsor and/or the plan, plan number and the EIN (or DLN).
b. Verify disclosure to determine authorization. See IRM 21.3.8.5.1.3.3, Status of Pending (Open) Employee Plans (EP) Determination/ Application Requests for more information.

10.10.3.3.14
(08-18-2023)
Identity Proofing for Employer Identification Number (EIN) Verification and Requests for Letter 147C, EIN Previously Assigned

(1) This subsections of the IRM provides guidance for Accounts Management Customer Service Representatives (CSR) and Non-Master-file Tax Examiners (TE) who answer BMF taxpayer inquiries (telephone, correspondence, or in person) and internal account requests. The subsections of the IRM is intended for Customer Account Services issues involving BMF tax returns. Once the relationship with the entity is established, ask the caller for the EIN. If the caller cannot provide the EIN, you must authenticate the caller's personal identity before researching for the EIN. The following identity proofing process will be used to authenticate the caller's identity:

a. Complete name
b. Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN)
c. Address
d. Date of Birth (DOB)

Use the following table to help you in authenticating the caller's information:

If	And	Then
The caller does not have an SSN/ITIN, or INOLEX is returned with limited information	Is not authenticated using CC INOLES	Disclose the EIN to the caller if their position with the entity authorizes them to receive it. See procedures in paragraph 2 below to research the entity information.

If	And	Then
The caller does not provide the correct address of record, but correctly responds to all other items, (Name, SSN/ ITIN, and date of birth)	You are unable to verify the address on CC INOLES	Request the address as it appears on the last tax return, or as modified by IRS records. • If address is verified, follow procedures in paragraph 2 below. • If the address is not verified, but you are confident the caller is who they say they are, follow the procedures in paragraph 2 below
The caller fails the DOB probe	Correctly responds to all other items above (Name, SSN/ITIN, and address)	Advise the caller to contact the Social Security Administration (SSA) at 800-722-1213, or *www.ssa.gov*, to correct the error. If you are confident the caller is who they say they are, continue with the call.

(2) When the relationship with the entity is established per paragraph 1, or the caller has provided the EIN, research for and/or verify the EIN using the correct command codes by obtaining the following information:

- EIN - (If known)
- Name of business - If the caller does not include the full name (e.g., LLC, INC, Corp, etc.) probe for more information.
- Address of business - If an address shows a possible typographical error, or is missing the suffix (e.g., STE, AVE, BLVD, etc.) probe for more information.

10.10.3.3.15
(08-18-2023)
Identity Proofing for Modernized Internet EIN (Mod IEIN)

(1) This subsections of the IRM provides guidance for Accounts Management Customer Service Representatives (CSR) and Non-Master-file Tax Examiners (TE) who answer BMF taxpayer inquiries (telephone, correspondence, or in person) and internal account requests. The IRM is intended for Customer Account Services issues involving BMF tax returns. The following table

includes the identity proofing process to use when authenticating a taxpayer or a POA/TIA calling the IRS regarding issues applying for their domestic or U.S. territory EIN online.

If the caller is:	And	Then
A POA/TIA	They can fax Form SS-4 signed by the responsible party along with Form 2848/Form 8821 with: • Form 2848/ Form 8821 notated with language such as application for an EIN, Form SS-4, etc.	Ask the POA/TIA to provide the following information. Their: • Name • Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN) • Address • Date of Birth Authenticate the POA/TIA by verifying their information using Command Code (CC) INOLES.
The taxpayer	Their position is authorized for the entity type. See IRM 21.7.13.5, Assigning EINs, for each specific entity type to determine if the caller's position is authorized for that entity type.	Ask the taxpayer to provide the following information. Their: • Name • Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN) • Address • Date of Birth Authenticate the caller by verifying their information using Command Code (CC) INOLES.

10.10.3.3.16
(08-18-2023)
Identity Proofing for Form SS-4 Application Status

(1) This subsections of the IRM provides guidance for Accounts Management Customer Service Representatives (CSR) and Non-Master-file Tax Examiners (TE) who answer BMF taxpayer inquiries (telephone, correspondence, or in person) and internal account requests. The IRM is intended for Customer Account Services issues involving BMF tax returns. Once the relationship with the entity is established and the caller is requesting to receive the EIN verbally, use the following identity proofing process to authenticate the caller's identity. Ask the caller for their:

a. Complete name

b. Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN)
c. Address
d. Date of Birth (DOB)

(2) Using the information provided by the caller, authenticate them using CC INOLES.

Caution: If the caller does not have an SSN/ITIN (and therefore cannot be authenticated using CC INOLE), or CC INOLEX is returned with limited information (DOB-Name Control), the new EIN may still be disclosed to the caller, as long as their position with the entity authorizes them to receive it.

(3) If the caller fails to provide the correct address of record but correctly responds to all of the other items (Name, SSN/ITIN and date of birth), request the address as it appears on the last tax return or as modified by IRS.

(4) If the caller fails the DOB probe but correctly responds to all other items above, (Name, SSN/ITIN, and address), advise them to contact the Social Security Administration (SSA) at 800-772-1213 or *www.ssa.gov* to correct the error. If you are confident the caller is who they say they are, continue with the call.

(5) When the relationship with the entity has been established and the caller has been authenticated, using the IAT EIN Assignment tool research the following information to determine if an EIN has been assigned:

1. Name of business
2. Address of business

Exception: Manually input the appropriate research CC's when the tool is unavailable.

10.10.3.4
(08-18-2023)
In-Person/Remote In-Person

(1) Frontline employees answer inquiries on the in-person or remote in-person channels for external communications. Taxpayers may be required or prefer to go to a local Taxpayer Assistance Center (TAC) to complete IRS transactions. At the TAC, they may be assisted by frontline employees through video conferencing. Procedures that align to the in-person/remote in-person channel are contained within the following sections.

10.10.3.4.1
(08-18-2023)
Identity Verification for TAC Disclosure Guidelines for ITIN Data

(1) This subsections of the IRM provides guidance for IRS employees in Austin Submission Processing Campus ITIN Operations, Accounts Management Customer Service Representatives, and Field Assistance. The following identity proofing process will be used when securing information from the customer to identify the specific application in question and compare the information provided to the information on RTS:

1. Name – Line 1a
2. Name at Birth – Line 1b, if different from Line 1a
3. Date of Birth – Line 4
4. Country of Birth – Line 4
5. Country of Citizenship – Line 6a

6. Previously issued ITIN or IRSN – Line 6e and Line 6f
7. Type of supporting documentation submitted

(2) If unable to verify the required fields, verify two or more additional entries from the application (for example, middle name, country issuing documentation, date of entry, or college name/city).

(3) You must also confirm the relationship of the customer to the applicant. The signature area of the W-7 Application View screen captures the name of the person signing Form W-7 as well as their relationship to the applicant. The following signature relationships are available on the RTS:

1. Applicant
2. Parent
3. Court Appointed Guardian
4. Power of Attorney
5. None

(4) Use the following table to determine appropriate disclosure actions:

If...	**Then...**	**Action**
Applicant,	Request documentation verifying identity (e.g., passport, driver's license, etc.),	If applicant provides appropriate documentation, continue contact. If applicant cannot provide appropriate documentation, advise applicant what is needed and to return to TAC with appropriate documentation.

If...	Then...	Action
Parent or Court Appointed Guardian,	Determine who signed the application and the age of the applicant. Request documentation to prove relationship to applicant.	If applicant is **under age 18**, their parent or court appointed guardian can sign if the child is unable to sign. The individual (if other than the applicant) must type or print their name in the space provided and indicate their relationship to the applicant. If the individual is a court appointed guardian, a copy of the court-appointment papers showing the legal guardianship must be presented. ***Caution:*** If an adult other than a parent or court appointed guardian signs for a minor child, they must have a Form 2848 from the parent or court appointed guardian authorizing them to sign. If the applicant is **18 years of age or older,** applicant may sign or appoint their parent, court appointed guardian or other individual to sign. The individual (if other than the applicant) must type or print their name in the space provided, indicate their relationship to the applicant and present Form 2848. ***Caution:*** A spouse may not sign for their husband or wife unless legal guardianship documents or a POA have been presented.

If...	Then...	Action
Authorized third-party	Determine if power of attorney (Form 2848, Power of Attorney and Declaration of Representative) or authorized party (Form 8821, Tax Information Authorization), or legal guardian (court documentation), ***Note:*** The Form 2848 or Form 8821 must state specifically that it is for an ITIN or Form W-7	If authorized third-party provides completed Form 2848 or Form 8821, continue contact. ***Caution:*** Form 8821 does not authorize the representative to sign the application on behalf of the applicant. The name of the third-party and the relationship to applicant must be indicated in the signature area of the Form W-7. If authorized third-party cannot provide the appropriate documentation, advise them what documentation is needed.
Independent entrepreneur, (someone other than applicant, authorized third-party, or parent is dropping off applications)		If application, supporting documentation, tax return or exception rule substantiation, and appropriate signature(s) are present, accept the application. Advise the customer the application will be forwarded for processing and the processing time. If required information is not present, advise what is required and to return to TAC once completed.

(5) The application may have been submitted by an Acceptance Agent. If the customer is the Acceptance Agent, verify their name and Employer Identification Number (EIN) by comparing the information that is on the RTS to the information provided.

Note: Acceptance Agents have a contractual agreement with the IRS to prepare Form W-7 and are **not** required to have power of attorney. This agreement is with the company and not individuals. Further verification is not required.

10.10.3.4.2
(08-18-2023)
Identity Verification for Virtual Service Delivery (VSD)

(1) This subsections of the IRM provides guidance for all Field Assistance employees, managers and analysts in TACs located in the United States and Puerto Rico. The following identity proofing process will be used when taxpayers are providing their TIN to TAC employees for VSD:
When requesting a Taxpayer Identification Number (TIN), ask the taxpayer to: hold their social security card or notice to the camera **OR** place it on the desk and point the camera down instead of speaking the number aloud.

10.10.3.4.3
(08-18-2023)
Identity Verification for Letter 5881-C or 5877-C Contacts

(1) This subsections of the IRM provides guidance for Customer Service Representatives (CSRs) and Customer Service Specialists (CSSs) in responding to telephone inquiries from Tax Exempt/Government Entities (TEGE) customers. The following identity proofing process will be used when taxpayers are providing personal identification to a TAC employee in response to a denial of an e-file application per Letter 5881C E-file Application Program Denial, Letter 5877C E-file Application IDT Sanction - Criminal Expulsion, or outdated Letter 2916:
To verify identity the customer must present two forms of ID:
An unexpired government issued photo ID, such as:

- Driver's license
- Passport
- State identification card OR
- Certified Birth Certificate

Note: These documents should **not** go through the document authentication process currently used to authenticate ITIN documents.

10.10.3.4.4
(08-18-2023)
Identity Verification for Preparing Returns Using Virtual VITA/TCE

(1) This subsections of the IRM provides guidance for all SPEC employees, managers, and analysts. The following identity proofing process will be used as part of the Virtual VITA/TCE process when a taxpayer presents photo identification at the intake site.
If the taxpayer(s) must return to the site, the taxpayer(s) must again supply photo identification when they return to review, sign, and pick up a copy of their return.

10.10.3.4.5
(08-18-2023)
Identity Verification for ITIN/SSN Mismatch Procedures

(1) This subsections of the IRM provides guidance for all SPEC employees, managers, and analysts. The following identity proofing process will be used when a taxpayer presents identification to a volunteer to prepare the tax return.

Note: Sites require two forms of identification. One photo identification such as:

- Passport
- National identity card
- Driver's license
- State identification card (U.S.)
- Military identification card
- School photo ID
- VISA

(2) The second form of identification needed is the original or a copy of the ITIN card or letter.

(3) One or both forms of identification must contain the taxpayer's current mailing address. If the taxpayer cannot prove their identity, or if the volunteer is uncomfortable accepting items presented as proof of identity, the volunteer must refer the taxpayer to obtain/seek professional tax help.

10.10.3.4.6
(08-18-2023)
Identity Verification for Quality Site Requirements (QSR)

(1) This subsections of the IRM provides guidance for all SPEC employees, managers, and analysts. The following identity proofing process will be used when the taxpayer, visiting VITA and TCE sites, presents identification to the coordinator to receive correct return preparation:

- Photo identification for primary and secondary taxpayers
- Social Security Numbers (SSN) or Individual Taxpayer Identification Numbers (ITIN) for everyone listed on the return.

10.10.3.5
(08-18-2023)
Digital/Online

(1) Frontline assistors answer inquiries on or about the digital/online channels for external communications. Procedures that align to the digital/online channel will be contained within the following sections. IRS frontline employees do not assist taxpayers who are navigating a Credential Service Provider's (CSP) identity verification process. Employees must refer the taxpayer to the CSP's help desk (phone or online) for assistance or visit *www.IRS.gov* for more information.

10.10.3.5.1
(08-18-2023)
Identity Proofing for Online Payment Agreement (OPA) for IMF Debts

(1) This subsection of the IRM provides guidance and procedures for all employees within LMSB, SBSE, TEGE and W&I Business Operating Divisions, who work with or have a need to know about systems/files/processes. The following identity proofing process will be used to ensure that the POA is authorized to represent their client in the OPA application:

- Taxpayer's SSN or ITIN
- Their Centralized Authorization File (CAF) number, and
- Either the six-digit Caller ID number from the taxpayer's notice or POA's signature date on Form 2848, Power of Attorney and Declaration of Representative.

This information is used to ensure that the POA is authorized to represent their client in the OPA application. If subsequent Forms 2848 have been filed by the POA, the POA signature date on the most recent Form 2848 will be required. All outstanding tax periods must be included on the most recently filed Form 2848, Power of Attorney and Declaration of Representative for the OPA application to process.

10.10.3.5.2
(08-18-2023)
Identity Proofing for Verification Issues for BMF OPA Users

(1) This subsection of the IRM provides guidance and procedures for all employees within LMSB, SBSE, TEGE and W&I Business Operating Divisions, who work with or have a need to know about systems/files/processes. The following identity proofing process will be used for BMF taxpayers (or their POAs) to verify their authority to establish an online agreement for the business. A BMF taxpayer or POA must provide:

a. The business EIN
b. The date the EIN was established (MM/YYYY)
c. The business address
d. The Caller ID number provided in their notice

10.10.3.5.3
(08-18-2023)
Identity Proofing for Secure Access eAuthentication

(1) This subsection of the IRM provides guidance and procedures for all employees within LMSB, SBSE, TEGE and W&I Business Operating Divisions, who work with or have a need to know about systems/files/processes. The following identity proofing will be used for existing Secure Access eAuthentication, users will enter their username and password PLUS a six-digit security code that will be sent to the phone number entered as part of the registration process or IRS2Go.

10.10.3.6
(08-18-2023)
Correspondence

(1) Frontline employees answer inquiries on the correspondence channel for external communications. Procedures aligning to the correspondence channel are contained within the following section/s.

10.10.3.6.1
(08-18-2023)
Identity Verification for Identity Theft General Documentation Requirements

(1) This subsection of the IRM provides guidance and procedures for Appeals technical employees. The taxpayer needs to provide information to substantiate documentation within 30 days for Individual Master File (IMF) cases. The following identity proofing process outlines the information needed:

a. **Authentication of Identity:** A copy of a valid U.S. federal or state government issued form of identification (examples include a driver's license, state identification card, social security card, or passport).

Note: IRS no longer accepts Puerto Rican birth certificates issued before July 1, 2010. Taxpayers with birth certificates issued before this date must get new documentation from the Puerto Rico Vital Statistics Record Office.

b. **Support for ID theft:** Form 14039 Identity Theft Affidavit (IMF) / Form 14039-B Business Identity Theft Affidavit (BMF) in certain situations (refer to IRM 25.23.9.7, Form 14039-B, Business Identity Theft Affidavit), or a copy of the police report indicating ID theft as the issue.

Note: The IRS affidavit for IMF taxpayers is also available in Spanish as Form 14039(Spanish Version) Identity Theft Affidavit (Spanish Version).