



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.10.3

APRIL 14, 2025

EFFECTIVE DATE

(04-14-2025)

PURPOSE

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

MATERIAL CHANGES

- (1) IRM 10.10.3.1, Program Scope and Objectives - IPU 24U0091 issued 01-17-2024 added exception for SB/SE examination employees; IPU 25U0021 issued 01-03-2025 spelled out business unit acronyms in (3) and deleted voice from Telephone/Voice service channel in (3) and (6) for clarity.
- (2) IRM 10.10.3.1.1, Background - IPU 25U0021 issued 01-03-2025 corrected reference in (1); deleted voice in (2) for clarity and consistency.
- (3) IRM 10.10.3.1.5, Terms - IPU 24U0091 issued 01-17-2024 updated Digital/Non-Digital to clarify authentication terms; IPU 25U0021 issued 01-03-2025 spelled out business unit acronyms in (3) and deleted voice from Telephone/Voice service channel in (3) and (6) for clarity.
- (4) IRM 10.10.3.1.6, Acronyms - IPU 24U0091 issued 01-17-2024 added ACSS, CSCO, CSR, DLN, FA, MFT, NDARA, PIN, SPEC, TEDS/EDS.
- (5) IRM 10.10.3.1.7, Related Resources - IPU 24U0091 issued 01-17-2024 added column for new IRM reference; deleted row for IRM 21.2.1.58.1 crossing over to IRM 10.10.3.5.3, Identity Proofing for Secure Access eAuthentication, since this subsection is now deleted.
- (6) IRM 10.10.3.3, Telephone - IPU 25U0021 issued 01-03-2025 deleted "Voice" from title to clarify and reflect availability of keypad entries instead of voice commands.
- (7) IRM 10.10.3.3.1, Identity Proofing for Disclosure Guidelines for ITIN Data - IPU 25U0021 issued 01-03-2025 removed the language "if different from Line 1a" from (1) 2nd bullet to align the AM IRM and Exhibit 3.21.263-3.
- (8) IRM 10.10.3.3.2, Identity Proofing for Disclosure Guidelines for Acceptance Agents - IPU 25U0021 issued 01-03-2025 updated authorized representative to responsible party and added authorization entitlements to (1) table and deleted Note since RTS and EHSS no longer used.
- (9) IRM 10.10.3.3.3, Identity Proofing for Additional Taxpayer Authentication for Collection Employees - IPU 24U0091 issued 01-17-2024 spelled out Field Assistance and revised language in (1) from collection employees will use the IAT Disclosure Tool to are suggested to use, added reference to IRM 5.19.1.2.8, Mandated IAT Tools.
- (10) IRM 10.10.3.3.4, Identity Proofing for Transfer Personal Identification Number (PIN) Acceptance - IPU 25U0021 issued 01-03-2025 added AM to (1) bullet list since the policy applies to AM employees too.
- (11) IRM 10.10.3.3.5, Identity Proofing for Communication Skills/Outgoing Calls - IPU 24U0091 issued 01-17-2024 added exception for SB/SE employees in Campus Examination/AUR Operations, and SB/SE Field Examination and SB/SE Field Collection to (1); added (2) to indicate a separate paragraph and corrected citation in (2)(c); IPU 25U0021 issued 01-03-2025 removed Communication Skills from title to accurately reflect content; revised **proper** to **required** in (1)(c) and added direction to provide name of taxpayer in (2)(a) when making outgoing calls.

- (12) IRM 10.10.3.3.6, Identity Proofing for Required Taxpayer Authentication - IPU 24U0091 issued 01-17-2024 added exception for SB/SE employees in Campus Examination/AUR Operations, and SB/SE Field Examination and SB/SE Field Collection to (1), replaced (2) bullet list with alpha list; corrected title of IRM 10.10.3.4.1 to add the word TAC in (2)(a); added Note in (2)(b) to probe for more information when not an exact match to be consistent with requirements from IRM 21.1.3.2.3; deleted Caution in (2)(b) to not confirm or deny information since this is for BMF authentication; replaced Note in (2)(c) if unable to verify address on IDRS with information on changing address; removed the words “you may” in (2)(c) and (d) for requesting additional taxpayer authentication if taxpayer fails to provide the correct DOB and address of record, but correctly responds to all of the other items; added reference to IRM 5.19.1.2.8 for mandated IAT tools for ACS employees in (2)(d) Reminder; Added Note with link to IMF Disclosure Job Aid to (2); Added (7) definition for abbreviated authentication; clarified language from you can verify to verify if available in (4). IPU 25U0021 issued 01-03-2025 added statement to (1) to refer back to original IRM for additional procedures; added direction if the current address does not match the address of record on IDRS; added link to IRM 11.3.2.4.10 for authenticating minors in (2)(d) Reminder; added direction when a basic authentication probe is missing to (2) Note; added (3) for direction on transfer PIN contacts; added clarifying language to (4) for first time filer authentication; added Note to (5)(b) for clarity on BMF calls when entity name is not an exact match; updated the word **items** to **probes** for clarity in (5)(c) and deleted (name and title) as that information is in IRM 21.1.3.2.3(1), Required Taxpayer Authentication; added (6) to provide direction on BMF sole proprietor inquiries; added the word abbreviated to (7) to clarify the process.
- (13) IRM 10.10.3.3.7, Identity Proofing for Additional Taxpayer Authentication - IPU 24U0091 issued 01-17-2024 removed first two sentences in (1) to clarify audience and added clarification that the IAT Disclosure Tool is recommended for ACS employees; IPU 25U0021 issued 01-03-2025 added TAS to (1) recommending use of the IAT tool and a link to the Exhibit 21.2.2-2, Accounts Management Mandated IAT Tools; added link to job aid for IMF high risk disclosure; corrected OUO restriction in (2) and (3); deleted first sentence from (4) Note directing the caller must answer all the questions since the tool has been enhanced to make this unnecessary.
- (14) IRM 10.10.3.3.8, Identity Proofing for Third-Party (Oral Disclosure Consent, (ODC)) Authentication - IPU 24U0091 issued 01-17-2024 added exception for SB/SE employees in Campus Examination/AUR Operations, and SB/SE Field Examination and SB/SE Field Collection to (1); clarified authentication requirements and added all verification items to bullet list.
- (15) IRM 10.10.3.3.9, Identity Proofing for Third-Party Designee Authentication - IPU 24U0091 issued 01-17-2024 added exception for SB/SE employees in Campus Examination/AUR Operations, and SB/SE Field Examination and SB/SE Field Collection to (1); removed citation to IRM 10.10.3.9 and clarified language in (3) to follow procedures in (1) above; IPU 25U0021 issued 01-03-2025 changed **asking for** to **obtaining** in (2) to clarify if designee has already provided required information; replaced TXMOD with any CC in (3) first bullet..
- (16) IRM 10.10.3.3.10, Identity Proofing for Oral Disclosure Consent/Oral TIA (Paperless F8821) - IPU 24U0091 issued 01-17-2024 added exception for SB/SE employees in Campus Examination/AUR Operations, and SB/SE Field Examination and SB/SE Field Collection to (1).
- (17) IRM 10.10.3.3.11, Identity Proofing for Interactive Voice Response - IPU 25U0021 issued 01-03-2025 added clarification to (1) callers can now either speak or enter their authentication data.
- (18) IRM 10.10.3.3.12, Identity Proofing for Issue and Entity Identification and Taxpayer Authentication Procedures - IPU 24U0091 issued 01-17-2024 added authentication procedures to (1) previously in IRM 21.3.8.4.1.5; replaced reference to IRM 21.3.8.4.1.5 to refer to (8) below in (1) Reminder; IPU 25U0021 issued 01-03-2025 added 6103 reference to (2); added direction to address bullet in (2) for

- verifying the pending application; moved examples in (2) Note to Examples; moved examples in (7) to be distinctive from text; deleted historical Form 5500 and corrected reference from (11) to (9) in (7) Caution.
- (19) IRM 10.10.3.3.15, Identity Proofing for Modernized Internet EIN (Mod IEIN) - IPU 25U0021 issued 01-03-2025 added note to (2) referring to IRM 21.7.1.4.7.1 if the taxpayer provides the EIN. Removed direction to show notice since TINs are no longer on notices.
 - (20) IRM 10.10.3.4, In-Person/Remote In-Person - Clarified audience to be inclusive of other functions that use in-person service channels.
 - (21) IRM 10.10.3.4.1, Identity Verification for In-Person Contacts - Added authentication policy for in-person contacts being removed from IRM 21.1.3.2.3.
 - (22) IRM 10.10.3.4.2, Identity Verification for Remote In-Person Contacts - IPU 24U0091 issued 01-17-2024 added Virtual VITA/TCE to (1) to include SPEC authentication. IPU 25U0021 issued 01-03-2025 retitled from Virtual Service Delivery (VSD) and removed notice from (1) table since TINs are no longer on notices; clarified language to be inclusive of other functions.
 - (23) IRM 10.10.3.4.2.1, Identity Verification for Subsequent In-Person Contacts - New policy to authenticate returning in-person contacts each time.
 - (24) IRM 10.10.3.4.3, Identity Verification for TAC Disclosure Guidelines for ITIN Data - IPU 25U0021 issued 01-03-2025 added reference to IRM 3.21.263.8.1 and IRM 3.21.263.7.1.1 to (1) for actions to take after authenticating.
 - (25) IRM 10.10.3.4.6, Identity Verification for Preparing Returns Using Virtual VITA/TCE - IPU 24U0091 issued 01-17-2024 spelled out SPEC acronym.
 - (26) IRM 10.10.3.5.1, Identity Proofing for Online Payment Agreement (OPA) for IMF Debts - IPU 24U0091 issued 01-17-2024 added exception for SB/SE employees in Campus Examination/AUR Operations, and SB/SE Field Examination and SB/SE Field Collection to (1).
 - (27) IRM 10.10.3.5.2, Identity Proofing for Verification Issues for BMF OPA Users - IPU 24U0091 issued 01-17-2024 added exception for SB/SE employees in Campus Examination/AUR Operations, and SB/SE Field Examination and SB/SE Field Collection to (1).
 - (28) IRM 10.10.3.5.3, Identity Proofing for Secure Access eAuthentication - IPU 24U0091 issued 01-17-2024 entire subsection removed due to revision made on 10-01-2023 for IRM 21.2.1.58.1 resulting in no crossover to the authentication policy.
 - (29) IRM 10.10.3.7, Multilingual Assistance and American Sign Language (ASL) Interpreters - IPU 25U0021 issued 01-03-2025 added information for authenticating foreign language and hearing impaired taxpayers.
 - (30) IRM 10.10.3 revised throughout with IPU 25U0021 issued 01-03-2025 to update organizational title Wage and Investment (W&I) to Taxpayer Services (TS).
 - (31) Editorial changes made throughout IRM with IPU 25U0021 issued 01-03-2025 for clarity, plain language, grammar, updates to titles, website addresses, legal and IRM references.

EFFECT ON OTHER DOCUMENTS

IRM 10.10.3 dated August 18, 2023 is superseded. The following IRM Procedural Updates (IPUs), issued on 01/17/2024 and 01/03/2025, have been incorporated into this IRM: 24U0091, 25U0021.

AUDIENCE

The primary audience is IRS employees in areas who interact with taxpayers by telephone, correspondence, face-to-face (in person or remote), or online communications. It does not include employees from SB/SE Campus Examination/AUR Operations and SB/SE Field Examination and SB/SE Field Collection whose current IRMs are not listed in the (3) crosswalk of IRM 10.10.3.1.7, Related Resources. Generally, if an IRM is in the related resource subsection and was used for identity proofing or verification, this IRM is now the official reference for authentication.

John E. Lyons
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 Program Scope and Objectives

- 10.10.3.1.1 Background
- 10.10.3.1.2 Authority
- 10.10.3.1.3 Roles and Responsibilities
- 10.10.3.1.4 Program Controls
- 10.10.3.1.5 Terms
- 10.10.3.1.6 Acronyms
- 10.10.3.1.7 Related Resources

10.10.3.2 Understanding Identity Proofing for Authentication

10.10.3.3 Telephone

- 10.10.3.3.1 Identity Proofing for Disclosure Guidelines for Individual Taxpayer Identification Number (ITIN) Data
- 10.10.3.3.2 Identity Proofing for Disclosure Guidelines for Acceptance Agents
- 10.10.3.3.3 Identity Proofing for Additional Taxpayer Authentication for Collection Employees
- 10.10.3.3.4 Identity Proofing for Transfer Personal Identification Number (PIN) Acceptance
- 10.10.3.3.5 Identity Proofing for Outgoing Calls
- 10.10.3.3.6 Identity Proofing for Required Taxpayer Authentication
- 10.10.3.3.7 Identity Proofing for Additional Taxpayer Authentication
- 10.10.3.3.8 Identity Proofing for Third-Party (Oral Disclosure Consent, (ODC)) Authentication
- 10.10.3.3.9 Identity Proofing for Third-Party Designee Authentication
- 10.10.3.3.10 Identity Proofing for Oral Disclosure Consent/Oral TIA (Paperless F8821)
- 10.10.3.3.11 Identity Proofing for Interactive Voice Response
- 10.10.3.3.12 Identity Proofing for Issue and Entity Identification and Taxpayer Authentication Procedures
- 10.10.3.3.13 Identity Proofing for Status of Pending (Open) Employee Plans (EP) Determination/Application Requests
- 10.10.3.3.14 Identity Proofing for Employer Identification Number (EIN) Verification and Requests for Letter 147C, EIN Previously Assigned
- 10.10.3.3.15 Identity Proofing for Modernized Internet EIN (Mod IEIN)
- 10.10.3.3.16 Identity Proofing for Form SS-4 Application Status

10.10.3.4 In-Person/Remote In-Person

- 10.10.3.4.1 Identity Verification for In-Person Contacts
- 10.10.3.4.2 Identity Verification for Remote In-Person Contacts
 - 10.10.3.4.2.1 Identity Verification for Subsequent In-Person Contacts
- 10.10.3.4.3 Identity Verification for TAC Disclosure Guidelines for ITIN Data
- 10.10.3.4.4 Identity Verification for Virtual Service Delivery (VSD)

-
- 10.10.3.4.5 Identity Verification for Letter 5881C or 5877C Contacts
 - 10.10.3.4.6 Identity Verification for Preparing Returns Using Virtual Volunteer Income Tax Assistance/Tax Counseling for the Elderly (VITA/TCE)
 - 10.10.3.4.7 Identity Verification for ITIN/SSN Mismatch Procedures
 - 10.10.3.4.8 Identity Verification for Quality Site Requirements (QSR)
 - 10.10.3.5 Digital/Online
 - 10.10.3.5.1 Identity Proofing for Online Payment Agreement (OPA) for IMF Debts
 - 10.10.3.5.2 Identity Proofing for Verification Issues for BMF OPA Users
 - 10.10.3.6 Correspondence
 - 10.10.3.6.1 Identity Verification for Identity Theft General Documentation Requirements
 - 10.10.3.7 Multilingual Assistance and American Sign Language (ASL) Interpreters

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

page 1

10.10.3.1
(01-03-2025)

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.
- (2) 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. Follows omni-channel best practices used across all IRS customer service applications, a recommendation in the IRS Authentication, Authorization, Access (A3) FY 2022 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.
- (3) **Audience:** IRS employees who are in contact with taxpayers through correspondence, telephone, in-person, remote in-person (video teleconferencing), and online exchanges. For example, Taxpayer Services (TS), Small Business/Self Employed (SB/SE), Large Business & International (LB&I), Taxpayer Advocate Service (TAS), and Independent Office of Appeals (Appeals).

Exception: Refer to the manual transmittal audience for specifically excluded SB/SE examination functions.

- (4) **Policy Owner:** Identity Assurance (IA), under Privacy Governmental Liaison and Disclosure (PGLD), is the program office responsible for oversight of the policy and procedures for identity verification and authentication.
- (5) **Program Owner:** The IA director reports to the chief privacy officer and is responsible for IA program oversight.
- (6) **Primary Stakeholders:** Management officials and employees within organizations and business units who authenticate taxpayers or representatives over

digital and non-digital channels (correspondence, telephone, in-person, remote in-person (video teleconferencing), and online exchanges).

- (7) **Program Goals:** Provide authentication guidance for Accounts Management (AM), 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
(01-03-2025)
Background

- (1) IRS employees must always verify the taxpayer's identity per IRM 11.3.1.2, Disclosure Code, Authority and Procedure (CAP), 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, in-person, remote in-person (video teleconferencing), and online exchanges) where sensitive information is exchanged with individuals.
- a. Non-digital channels: correspondence, telephone, in-person/remote in-person assistance.
 - b. 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)
Roles and Responsibilities

- (1) The IA Director, within 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.
- (2) IA's role is to strengthen and implement IRS authentication standards for:
- Identity proofing,
 - Authentication,
 - Authorization, and
 - Access strategies, processes, and capabilities.
- (3) Part 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

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

page 3

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 IRS 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. Refer to Form 15295, Non-Digital Authentication Risk Assessment (NDARA). The Identity Assurance function manages and reviews authentication in Digital and Non-Digital Channels 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.
- (2) 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 AM, Campus Compliance, Field Assistance (FA), Tax Exempt/Government Entities (TE/GE), Return Integrity and Compliance Services (RICS), and Electronic Products and Services Support (EPSS).

10.10.3.1.5 (01-03-2025) 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. For example businesses and 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 the IRS interacts with external stakeholders.
Correspondence (mail, fax)	Communications through mail and fax.
Digital Authentication	Online services/applications including website and mobile applications.
Disclosure	Making known the return or return information to any person in any manner.
Identity Assurance (IA)	A function within PGLD 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 location or use video conferencing to provide in-person/remote in-person identity proofing or authentication with an identification document, such as a driver's license.
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 Authentication	Correspondence, telephone, in-person/remote in-person assistance.
Telephone	Enterprise Architecture approved telephone and voice channels for external communications.

10.10.3.1.6
(01-17-2024)

Acronyms

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

Acronym	Definition
A3	Authentication, Authorization and Access
AAL	Authenticator Assurance Level
ACS	Automated Collection System
ACSS	Automated Collection System Support
AMS	Account Management Services
AOR	Address of Record
BMF	Business Master File
CAF	Centralized Authorization File

Acronym	Definition
CC	Command Code
CSCO	Compliance Services Collection Operations
CSR	Customer Service Representative
DBA	"Doing Business As"
DLN	Document Locator Number
DOB	Date of Birth
EFIN	Electronic Filer Identification Number
EHSS	E-help Support System
EIN	Employer Identification Number
EQ	Embedded Quality
FA	Field Assistance
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
MFT	Master File Tax
MOD IEIN	Modernized Internet Employer Identification Number
NDARA	Non-Digital Authentication Risk Assessment
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
PIN	Personal Identification Number

Acronym	Definition
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
RTS	Real-Time System
SBU	Sensitive But Unclassified
SPEC	Stakeholder Partnerships, Education and Communication
SSN	Social Security Number
TAC	Taxpayer Assistance Center
TCE	Tax Counseling for the Elderly
TEDS/EDS	Tax Examination Determination System/Exempt Determination System
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
(01-17-2024)

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 800-63A guidelines
 - IRM 10.5.1, Privacy Policy
 - IRM 10.5.4, Incident Management Program
 - IRM 10.5.5, Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements
 - IRM 11.3.1, Introduction to Disclosure
- (2) In the event an inadvertent disclosure occurs or an unauthorized access takes place, refer to the following guidance:
 - IRM 10.5.1, Privacy Policy
 - IRM 10.5.4, Incident Management Program
 - IRM 10.5.5, Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements
 - IRM 11.3.1, Introduction to Disclosure

(3) The following table lists the primary sources of guidance:

Previous IRM that contained the authentication policy	Previous IRM title that contained the authentication policy	Channel	Current IRM that contains the authentication policy
IRM 3.21.263.7.1.1	TAC Disclosure Guidelines for ITIN Data	In-Person	IRM 10.10.3.4.3
IRM 3.21.263.8.1	Disclosure Guidelines for ITIN Data	Phone	IRM 10.10.3.3.1
IRM 3.21.264.3.3	Disclosure Guidelines for Acceptance Agents	Phone	IRM 10.10.3.3.2
IRM 5.19.1.2.3.2	Additional Taxpayer Authentication	Phone	IRM 10.10.3.3.3
IRM 5.19.1.2.3.3.1	Transfer Personal Identification Number (PIN) Acceptance	Phone	IRM 10.10.3.3.4
IRM 8.6.5.2	Identity Theft General Documentation Requirements	Correspondence	IRM 10.10.3.6.1
IRM 21.1.1.4	Communication Skills	Phone	IRM 10.10.3.3.5
IRM 21.1.3.2.3	Required Taxpayer Authentication	Phone	IRM 10.10.3.3.6
IRM 21.1.3.2.4	Additional Taxpayer Authentication	Phone	IRM 10.10.3.3.7
IRM 21.1.3.3	Third-Party (POA/TIA/F706) Authentication	Phone	IRM 10.10.3.3.8
IRM 21.1.3.3.1	Third-Party Designee Authentication	Phone	IRM 10.10.3.3.9
IRM 21.1.3.3.2	Oral Disclosure Consent/Oral TIA (Paperless F8821)	Phone	IRM 10.10.3.3.10
IRM 21.2.1.57	Online Payment Agreement (OPA) for IMF Debts	Online	IRM 10.10.3.5.1
IRM 21.2.1.57.1.1	Verification Issues for BMF OPA Users	Online	IRM 10.10.3.5.2
IRM 21.2.3.3.3	Interactive Voice Response	Phone	IRM 10.10.3.3.11
IRM 21.3.4.2.3	Virtual Service Delivery (VSD)	In-Person/ Remote In-Person	IRM 10.10.3.4.4
IRM 21.3.4.26.1	Letter 5881C or 5877C Contacts	In-Person	IRM 10.10.3.4.5

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

page 9

Previous IRM that contained the authentication policy	Previous IRM title that contained the authentication policy	Channel	Current IRM that contains the authentication policy
IRM 21.3.8.4.1.5	Issue and Entity Identification and Taxpayer Authentication Procedures	Phone	IRM 10.10.3.3.12
IRM 21.3.8.5.1.3.3	Status of Pending (Open) Employee Plans (EP) Determination/ Application Requests	Phone	IRM 10.10.3.3.13
IRM 21.7.1.4.7.1	Employer Identification Number (EIN) Verification and Requests for Letter 147C, EIN Previously Assigned	Phone	IRM 10.10.3.3.14
IRM 21.7.13.3.4.1	Modernized Internet EIN (Mod IEIN)	Phone	IRM 10.10.3.3.15
IRM 21.7.13.3.9.1	Form SS-4 Application Status	Phone	IRM 10.10.3.3.16
IRM 22.30.1.8.1.1.3	Preparing Returns Using Virtual VITA/TCE	In-Person	IRM 10.10.3.4.6
IRM 22.30.1.8.9.4.1.1	Individual Taxpayer Identification Number/ Social Security Number “SSN/ITIN Mismatch”	In-Person	IRM 10.10.3.4.7
IRM 22.30.1.8.12.1	Quality Site Requirements (QSR)	In-Person	IRM 10.10.3.4.8

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.
- (2) The following subsections cover procedures that are handled through a variety of IRS channels. These channels include correspondence, telephone, in-person, remote in-person (video teleconferencing), and online exchanges. The procedures consolidated in this IRM have been broken down into subsections by IRS channel.

10.10.3.3 (01-03-2025) **Telephone**

- (1) Frontline employees engage in external communications via telephone and voice channels. Procedures for telephone and voice channels are contained throughout the following subsections.
- (2) Prior to providing authorized tax return information, ask for identifying information and conduct IDRS research to validate the responses. For example, name

and taxpayer identification number (TIN). For a list of the research command codes, refer to IRM 21.1.3.2.3(11), Required Taxpayer Authentication, for additional information.

10.10.3.3.1
(01-03-2025)

**Identity Proofing for
Disclosure Guidelines
for Individual Taxpayer
Identification Number
(ITIN) Data**

- (1) This subsection of the IRM provides guidance and procedures for IRS employees in:

- Austin Submission Processing Campus Individual Taxpayer Identification Number (ITIN) Operations
- AM Customer Service Representatives (CSRs)
- 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
- Date of birth (DOB) – 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.

If	Then
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 guardian's name is in the "Name of delegate" field. Compare this to the information provided by the caller.

If	Then
<p>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.</p>	<p>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:</p> <p>Caution: If a Form 2848 was submitted after the original Form W-7 was processed, the POA name is recorded in the Remarks Screen.</p> <ul style="list-style-type: none"> • If in Suspense (S 14) Status, advise the caller to resubmit the documents to the Austin ITIN Unit • For any other status, refer to IRM 21.1.3.3, Third-Party (POA/TIA/F706) Authentication, if no Form 2848 is found. Refer to 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, provide the International AM 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 inquiring about the status of an application, refer them to their signed CAA agreement and have them call the number listed in the agreement.

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

page 13

10.10.3.3.2 (01-03-2025) 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 tables to authenticate a customer and their authority to receive information about an Acceptance Agent application:

Position/ Relationship	Authentication Requirements	Authorization Entitlements
Principal, Partner, or Owner	EIN, legal or DBA name, physical or mailing address	Application status, firm suitability or tax compliance issue
Responsible Party (U.S. Citizen)	Social Security number (SSN), name, address, filing status as shown on last return, and DOB	Application status and individual suitability
Responsible Party (non-resident alien)	PTIN, name, address, DOB	Application status and individual suitability
Responsible Party (foreign national)	PTIN, name, address, DOB (CC RPVUE for foreign nationals)	Application status and individual suitability
Primary or Alternate Contact	EIN, title, phone number, email address	General information

10.10.3.3.3 (01-17-2024) Identity Proofing for Additional Taxpayer Authentication for Collection Employees

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

- ACS and ACSS
- CSCO
- FA

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 are suggested to use this tool to assist in verifying the identity of a caller and determining if the caller is authorized to receive confidential tax information or represent the taxpayer. Refer to IRM 5.19.1.2.8, Mandated IAT Tools. There will be times when systemic issues cause problems with the IAT Disclosure tool 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. For Individual Master File (IMF) accounts:

- a. Filing status on return in question.
- b. Spouse's date of birth.
- c. Child's/children's date(s) of birth.
- d. Amount of income reported on last return or tax due on return.
- e. Employers shown on taxpayer's Form W-2.

- f. Financial institutions from taxpayer's Form 1099-INT or Form 1099-DIV.
- g. Number of exemptions claimed on last return or on return in question.
- h. Preparer, paid/unpaid, if any.
- i. Expected refund amount (within \$100) **unless** computed by IRS.
- j. 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 can be easily discoverable or guessed.

For Business Master File (BMF) accounts:

- a. Federal income tax withheld/Social Security wages Form 941.
- b. Gross receipts or sales/Taxable income Form 1120.
- c. Total assets/Total liabilities Form 990.
- d. 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 can be easily discoverable or guessed.

10.10.3.3.4
(01-03-2025)
**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,
- AM employees and
- FA employees.

Taxpayers may inform an IRS assistor they have a four (4) digit transfer personal identification number (PIN) provided by the previous IRS assistor. When this occurs, 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 is only used by taxpayers. If a third party attempts to use a transfer PIN, **do not** accept it. Instead refer to IRM 5.19.1.2.3.3.1(5), Transfer Personal Identification Number (PIN) Acceptance.

10.10.3.3.5
(01-03-2025)
**Identity Proofing for
Outgoing Calls**

- (1) This subsection of the IRM provides guidance for Taxpayer Services (TS) and Small Business/Self Employed (SB/SE) business operating divisions (except employees in SB/SE Campus Examination/AUR Operations and SB/SE Field Examination and SB/SE Field Collection), that 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 required.

- (2) Use the following identity proofing process when verifying the requestor's identity for when you initiate an outgoing phone call. The taxpayer may be reluctant to give you their TIN:

- a. Provide the name of the taxpayer and the last four digits of their TIN (SSN/EIN).
- 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 10.10.3.3.6, Identity Proofing for Required Taxpayer Authentication.

10.10.3.3.6
(01-03-2025)
**Identity Proofing for
Required Taxpayer
Authentication**

- (1) This subsection provides guidance for all IRS employees, in business operating divisions, 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 (except employees in SB/SE Campus Examination/AUR Operations and SB/SE Field Examination and SB/SE Field Collection), TE/GE, TAS and TS. IRM 10.10.3 contains authentication policy only and provides the identity proofing steps involved for each service channel included. However, for specific details or procedural guidelines, refer back to your original IRM.

- (2) Use the following identity proofing process to verify the requestor's identity for required IMF authentication probes. Obtain and validate the correctness of:
 - a. 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 is required if the primary is unavailable or can be used as an additional authentication check. Refer to 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 TAC 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.

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

Note: It is necessary to probe the caller for more information if the response provided is similar but not an exact match. For example, the response is missing information but you are certain that the correct account has been accessed. At the conclusion of all the required basic authentication probes, make the determination to either authenticate the caller or perform additional authentication if necessary.

- c. Current address – If the current address does not match the address of record on IDRS, request the address as it appears on the last tax return or as modified by IRS records. If the 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), request additional taxpayer authentication per IRM 10.10.3.3.7, Identity Proofing for Additional Taxpayer Authentication.

Note: If an address change is necessary, refer to IRM 21.1.3.20.1, IMF and BMF Oral Statement Address Changes, or IRM 3.13.5.29, Oral Statement/Telephone Contact Address Change Requirements.

- d. Date of birth 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), request additional taxpayer authentication per 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 that you are speaking with the correct taxpayer (caller passed authentication requirements), advise the taxpayer to contact the 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: Refer to Exhibit 21.2.2-2, Accounts Management Mandated IAT Tools, for those employees mandated to use *IAT Disclosure Tool*. For ACS employees, refer to IRM 5.19.1.2.8, Mandated IAT Tools. For authenticating minors, refer to IRM 11.3.2.4.10, Minors.

Note: If any information needed to verify a basic authentication probe is missing, it is considered a failed response and additional authentication is required. Do not confirm or deny any information until authentication is complete. For additional guidance and case examples for phone assistants conducting basic authentication on an IMF call, refer to the *SERP - Basic IMF Disclosure - Job Aids* (irs.gov) for assistance. You can make suggestions for improvements (changes or updates) to the job aid by submitting SERP feedback.

- (3) If applicable, refer to IRM 21.1.3.2.6, Accepting Transferred Calls When the Taxpayer Provides a 4-Digit Transfer PIN.
- (4) For first time filers, if the return is not completely processed or rejected, there could be limited entity information. Continue performing required IMF authentication probes in (2) above and verify, if available:
 - Amount of refund and filing status on CC FFINQ
 - Name Control and DOB on CC INOLES
 - Complete Name and DOB on CC DDBKD
- (5) For required BMF authentication probes, request the following information:
 - 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. Refer to 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 a 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. Refer to 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.

Note: It is necessary to probe the caller for more information if the BMF name provided is similar but not an exact match. For example, the response is missing information but you are certain that the correct account has been accessed. At the conclusion of all the required BMF authentication probes, the determination is made to either authenticate the caller or perform additional authentication if necessary.

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 the taxpayer fails to provide the correct address of record, but correctly responds to all of the other probes, request additional taxpayer authentication per 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, United States Gift Tax Return, (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, U.S. Estate Tax Return, (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 can use AMS Privacy and Disclosure screens to access IDRS.

- (6) After satisfactory authentication, provide the information requested. Once authentication is complete for a BMF sole proprietor inquiry, it is not necessary to re-authenticate if the caller has an IMF inquiry and the IMF entity data indicates the same name and address.

Note: This would also pertain if an IMF inquiry call was received first and authentication was complete, it would not be necessary to re-authenticate for a BMF sole proprietor inquiry.

- (7) Abbreviated authentication - only used after establishing the third-party authorization is valid for the account. You must validate the POA/TIA by verifying the caller's TIN (SSN or ITIN) and DOB. The POA/TIA must pass abbreviated authentication on their SSN to be validated as an authorized third-party. Refer to IRM 21.1.3.3, Third-Party (POA/TIA/F706) Authentication, for two exceptions to this policy.

10.10.3.3.7
(01-03-2025)
**Identity Proofing for
Additional Taxpayer
Authentication**

- (1) The following identity proofing process will be followed when employees are conducting additional taxpayer authentication. If conditions require additional taxpayer authentication, the use of the *IAT Disclosure Tool* is mandated (recommended for ACS and TAS employees). If the tool is down, then manual authentication is required. Refer to IRM 21.2.2-2, Accounts Management Mandated IAT Tools.

Note: Employees working the Taxpayer Protection Program (TPP) follow authentication procedures in IRM 25.25.6.4(8), 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, 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, 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 can 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 the year

#

mandated for the Taxpayer Protection Line. Refer to the SERP Job Aid for *High Risk IMF Disclosure*.

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, 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 not be
- 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 will 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: 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 could require some manual research since data pulled from the primary on some command codes are unique to that SSN (for example, 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 could be multiple responses in the answer portion such as the SSN and DOB 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 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 could 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 (01-17-2024) 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 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 (with the exception of employees in SB/SE Campus Examination/AUR Operations and SB/SE Field Examination and SB/SE Field Collection), TE/GE, TAS and TS.

- (2) Request and verify the following identity proofing information when authenticating the oral disclosure consent designee.

- Taxpayer's name
- Taxpayer's TIN
- Third-party name
- Third-party phone number
- Applicable tax form
- Applicable tax period

10.10.3.3.9
(01-03-2025)

**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 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 (except employees in SB/SE Campus Examination/AUR Operations and SB/SE Field Examination and SB/SE Field Collection), TE/GE, TAS and TS.

- (2) 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 obtaining:

- 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 the revocation.

- (3) 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 any CC shown in (1) above.
- 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.

- (4) 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 (follow the procedures in (1) above). 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
(01-17-2024)

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 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 (with the exception of employees in SB/SE Campus Examination/AUR Operations and SB/SE Field Examination and SB/SE Field Collection), TE/GE, TAS and TS.
- (2) 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
(01-03-2025)

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 returns and tax account transcripts. Taxpayers are prompted to enter or speak their:
 - SSN or ITIN.
 - Numbers/digits in the street address currently on file.

For more information on IVR, please refer to IRM 21.2.3.3.4, Interactive Voice Response.

10.10.3.3.12
(01-03-2025)

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 TE/GE Customer Account Services (CAS).
- (2) Identify the caller's issue and provide the information IF they are entitled under IRC 6103. If the caller does not provide enough information to determine the next steps, ask probing questions to determine whether the caller has a general question (one that can be answered without specific entity/plan sponsor/information) or whether the question is about a specific organization/plan. Do not treat a question relating to a **specific** organization/plan sponsor/plan as a need to authenticate the caller. Information open to public disclosure under IRC 6104 may be provided.

Example: If the caller states they want to check on the exempt status of an organization, proceed with identifying the organization and researching its

status. If the organization is in status 01, you may affirm the organization's exemption without having asked the caller's relationship to the organization.

Whenever the caller's question or issue concerns a specific organization or plan sponsor/plan, it is critical that the caller and the assistor are referring to the same organization or plan sponsor/plan. Ask the caller for:

- Name,
- Address (verify the address of record or address as listed on the pending application), 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 shown below*), disregard minor discrepancies in the name or address of the entity, **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.

Example: Omission of "INC" from the organization's name, "suite" instead of "apartment", "street" instead of "avenue" or the omission of a building name.

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 (8) below.

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.

- (3) 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 only have 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. In other words, 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 they were 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.

- (4) There are limitations to the research you can perform when the caller cannot provide enough information:
 - a. 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.
 - b. 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.
- (5) 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 can 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 entity to update their address.

- (6) 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.

- (7) 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.

Example: "I am the president of our local PTA and I want to check on the status of our application for exemption."

Using a purpose statement before asking the caller the disclosure prompts can help put the caller at ease and make you feel more comfortable asking the disclosure prompts.

Example: "In order to protect the organization and the IRS, I need to verify your relationship with the organization before disclosing certain information."

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. Refer to 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-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). Refer to (9) below if the caller is attempting to demonstrate authority and is unable to give the correct address of record for the appropriate Master File account.

- (8) 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 an exempt organization and employee plan disclosures 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.

- a. If the caller represents a government entity, refer to IRM 21.3.8.4.4.2, Instrumentality/Governmental Units Disclosure, for additional information.
- b. If the caller is a plan participant seeking information pertaining to a plan, refer to IRM 21.3.8.4.1.5.1, Authorization Requirements for Participants in an Employer-Sponsored Plan.
- c. Refer to 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 could be an outside third party who is not authorized without specific authority.

- d. 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.

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

- (9) 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.

- (10) 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.
- (11) Before an outside third party (accountant, bookkeeper, attorney) can be considered as authorized to receive information protected under IRC 6103, disclosure rules require:
 - a. Formal execution of authorization (Form 8821/Form 2848),
 - b. Oral consent by an authorized party (for specific account matters) **or**
 - c. 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 subsection provides guidance for CSRs and customer service specialists (CSSs) in responding to telephone inquiries from TE/GE 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 document locator number (DLN).
 - b. Verify disclosure to determine authorization. Refer to 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 subsection provides guidance for AM CSR and Non-Master-file Tax Examiners (TE) who answer BMF taxpayer inquiries (telephone, correspondence, or in person) and internal account requests. The subsection of the IRM is intended for CAS issues involving BMF tax returns.
- (2) 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. SSN or ITIN
 - c. Address
 - d. 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. Refer to procedures in (3) below to research the entity information.

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

page 27

If	And	Then
The caller does not provide the correct address of record, but correctly responds to all other items, (Name, SSN/ITIN, and DOB).	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. <ul style="list-style-type: none"> If the address is verified, follow procedures in (3) below. If the address is not verified, but you are confident the caller is who they say they are, follow the procedures in (3) below.
The caller fails the DOB probe.	Correctly responds to all other items above (Name, SSN/ITIN, and address).	Advise the caller to contact 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.

(3) When the relationship with the entity is established per (2) above, 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 (LLC, INC, Corp, etc.) probe for more information.
- Address of business - If an address shows a possible typographical error or is missing the suffix (STE, AVE, BLVD, etc.) probe for more information.

10.10.3.3.15 (01-03-2025) Identity Proofing for Modernized Internet EIN (Mod IEIN)

- (1) This subsection provides guidance for AM CSR and Non-Master-file tax examiners (TE) who answer BMF taxpayer inquiries (telephone, correspondence, or in person) and internal account requests. The subsection of the IRM is intended for CAS issues involving BMF tax returns.
- (2) 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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. Refer to 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: <ul style="list-style-type: none"> Name Social Security number (SSN) or individual taxpayer identification number (ITIN) Address Date of Birth Authenticate the caller by verifying their information using CC INOLES.

Note: If the taxpayer provides the EIN, refer to IRM 21.7.1.4.7.1, Employer Identification Number (EIN) Verification and Requests for Letter 147C, EIN Previously Assigned.

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

- (1) This subsection provides guidance for AM CSR and Non-Master-file TEs who answer BMF taxpayer inquiries (telephone, correspondence, or in person) and internal account requests. This subsection IRM is intended for CAS issues involving BMF tax returns.
- (2) 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. SSN or ITIN
 - c. Address
 - d. DOB

- (3) 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 can still be disclosed to the caller, as long as their position with the entity authorizes them to receive it.

- (4) If the caller fails to provide the correct address of record but correctly responds to all of the other items (Name, SSN/ITIN and DOB), request the address as it appears on the last tax return or as modified by IRS.
- (5) If the caller fails the DOB probe but correctly responds to all other items above (name, SSN/ITIN, and address), advise them to contact 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.
- (6) 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
(04-14-2025)
**In-Person/Remote
In-Person**

- (1) Taxpayers may prefer or be required to conduct IRS business at a local office or at an IRS approved alternate location. The following procedures apply to IRS employees and IRS authorized volunteers that meet with taxpayers in-person or via a remote in-person channel. These procedures do not apply to SB/SE Field Examination.

10.10.3.4.1
(04-14-2025)
**Identity Verification for
In-Person Contacts**

- (1) Request the taxpayer provide their TIN in writing or verbally. For Field Assistance, see IRM 21.3.4.3.6, Numeric Keypads.
- (2) For all individual in-person contacts, obtain a valid, unexpired, government issued photo identification (ID) to verify the identity of the taxpayer, if not already provided. Verify the photo ID matches the individual and their name, address and DOB on IRS records. If ID does not have the correct address of record, but all other items are verified, (IMF – name, TIN and date of birth), ask the taxpayer to verify the address on the last tax return filed.
- (3) If you are unable to verify with a photo ID or the taxpayer does not have a valid photo ID, proceed with additional taxpayer authentication in IRM 10.10.3.3.7, Identity Proofing for Additional Taxpayer Authentication.
- For required IMF and BMF authentication probes, refer to IRM 10.10.3.3.6, Identity Proofing for Required Taxpayer Authentication.
 - For third-party authentication, refer to IRM 21.1.3.3, Third-Party (POA/TIA/F706) Authentication.

Note: Refer to IRM 21.1.3.2.3, Required Taxpayer Authentication, for the procedures used to validate the contact.

10.10.3.4.2
(04-14-2025)

**Identity Verification for
Remote In-Person
Contacts**

- (1) This subsection of the IRM provides guidance for all IRS employees and IRS authorized volunteers that meet with taxpayers and/or their representatives using a remote in-person channel (IRS approved video conferencing).
- (2) Ask the taxpayer to position in front of the camera:
 - A social security card to verify their TIN, and
 - A valid, unexpired government issued photo identification (ID).
- (3) If the taxpayer does not have a card with their TIN, request the number be provided verbally or have the taxpayer write down the number and position in front of the camera.
- (4) Verify the photo ID matches the individual. Make sure their name, address and DOB on the ID matches IRS records. If the ID does not have the correct address of record, but all other items are verified, (IMF – name, TIN and date of birth), ask the taxpayer to verify the address on the last tax return filed. If the taxpayer fails to provide the correct address of record, request additional taxpayer authentication per IRM 10.10.3.3.7, Identity Proofing for Additional Taxpayer Authentication.
- (5) If the taxpayer does not have a photo ID, proceed with the required taxpayer authentication in IRM 10.10.3.3.6, Identity Proofing for Required Taxpayer Authentication, and IRM 10.10.3.3.7, Identity Proofing for Additional Taxpayer Authentication.
- (6) For third-party authentication, refer to IRM 21.1.3.3, Third-Party (POA, TIA, F706) Authentication.

10.10.3.4.2.1
(04-14-2025)

**Identity Verification for
Subsequent In-Person
Contacts**

- (1) If you meet with a taxpayer in-person or remotely (IRS approved video conferencing) on more than one occasion, verify the taxpayer's identity per IRM 10.10.3.4.1, Identity Verification for In-Person Contacts.

10.10.3.4.3
(01-03-2025)

**Identity Verification for
TAC Disclosure
Guidelines for ITIN Data**

- (1) This subsection provides guidance for IRS employees in Austin Submission Processing Campus ITIN Operations, AM CSRs, and FA.

Note: For actions to take after authentication, refer to IRM 3.21.263.8.1, Disclosure Guidelines for ITIN Data, or IRM 3.21.263.7.1.1, TAC Disclosure Guidelines for ITIN Data.
- (2) The following identity proofing process is used to identify the specific application in question and compare the information provided to the information on RTS:
 - Name – Line 1a
 - Name at birth – Line 1b
 - Date of birth (DOB) – 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
- (3) 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).
- (4) You must 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:
- a. Applicant
 - b. Parent
 - c. Court Appointed Guardian
 - d. Power of Attorney
 - e. None
- (5) Use the following table to determine appropriate disclosure actions:

If	Then	Action
Applicant,	Request documentation verifying identity (for example, passport, driver's license, etc.).	If the applicant provides appropriate documentation, continue contact. If the 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 the applicant.	<p>If the 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.</p> <p>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.</p> <p>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.</p> <p>Caution: A spouse may not sign for the other spouse unless legal guardianship documents or a POA have been presented.</p>

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

page 33

If	Then	Action
Authorized third-party,	Determine if the third party has a signed 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 the authorized third-party provides a 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 the authorized third-party cannot provide the appropriate documentation, advise them what documentation is needed.
Independent entrepreneur, (someone other than the applicant, authorized third-party, or parent is dropping off applications)	N/A	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.

- (6) The application may have been submitted by an acceptance agent. If the customer is the acceptance agent, verify their name and EIN by comparing the information that is on 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.

10.10.3.4.4
(01-03-2025)

Identity Verification for Virtual Service Delivery (VSD)

- (1) This subsection provides guidance for all FA employees and managers in TACs and for virtual Volunteer Income Tax Assistance/Tax Counseling for the Elderly (VITA/TCE) locations. The following identity proofing process will be used when taxpayers are providing their TIN. When requesting a TIN, ask the taxpayer to:
1. Hold their Social Security card to the camera, OR
 2. Place it on the desk and point the camera down instead of speaking the number aloud.

10.10.3.4.5
(08-18-2023)

**Identity Verification for
Letter 5881C or 5877C
Contacts**

- (1) This subsection provides guidance for CSRs and CSSs in responding to telephone inquiries from TE/GE customers.
- (2) 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
- AND either a
- Social Security Card OR
- Certified Birth Certificate

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

10.10.3.4.6
(01-17-2024)

**Identity Verification for
Preparing Returns Using
Virtual Volunteer Income
Tax Assistance/Tax
Counseling for the
Elderly (VITA/TCE)**

- (1) This subsection provides guidance for all Stakeholder Partnerships, Education and Communication (SPEC) employees and managers. 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.

10.10.3.4.7
(08-18-2023)

**Identity Verification for
ITIN/SSN Mismatch
Procedures**

- (1) This subsection 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.

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

page 35

10.10.3.4.8
(08-18-2023)
**Identity Verification for
Quality Site
Requirements (QSR)**

- (1) This subsection 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.
 - SSN or ITIN for everyone listed on the return.

10.10.3.5
(08-18-2023)
Digital/Online

- (1) Frontline assistants answer inquiries on or about the digital/online channels for external communications. Procedures that align to the digital/online channel are contained within the following subsections. 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
(01-17-2024)
**Identity Proofing for
Online Payment
Agreement (OPA) for
IMF Debts**

- (1) This subsection of the IRM provides guidance and procedures for all employees within LB&I, SB/SE (except employees in SB/SE Campus Examination/AUR Operations and SB/SE Field Examination and SB/SE Field Collection), TE/GE and TS business operating divisions, who work with or have a need to know about systems/files/processes.
- (2) 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,
 - POA's 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 Form 2848s 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
(01-17-2024)
**Identity Proofing for
Verification Issues for
BMF OPA Users**

- (1) This subsection of the IRM provides guidance and procedures for all employees within LB&I, SB/SE (with the exception of employees in SB/SE Campus Examination/AUR Operations and SB/SE Field Examination and SB/SE Field Collection), TE/GE and TS business operating divisions, who work with or have a need to know about systems/files/processes.
- (2) 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

10.10.3.6
(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 subsection.

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 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: The 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 (SP), Identity Theft Affidavit (Spanish Version).

10.10.3.7
(01-03-2025)
**Multilingual Assistance
and American Sign
Language (ASL)
Interpreters**

- (1) Authenticate taxpayers that use authorized interpreters as if you were talking to the taxpayer. Authentication through an authorized interpreter is allowed by following the established guidelines for securing an interpreter. For more information, refer to:

In-person/remote in-person	Telephone
IRM 21.3.4.2.4.5.4, Sign Language Interpreters	IRM 21.1.1.5, Over the Phone Interpreter (OPI) Service Applications
IRM 21.3.4.3.4, Multilingual Assistance	IRM 21.2.1.56, Deaf/Hard of Hearing (DHOH) Callers and TTY/TDD Equipment