



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

25.23.12

AUGUST 26, 2025

EFFECTIVE DATE

(10-01-2025)

PURPOSE

- (1) This transmits revised IRM 25.23.12, Identity Protection and Victim Assistance, IMF Identity Theft Toll-Free Guidance.

MATERIAL CHANGES

- (1) IRM 25.23.12.1 Updated TS to Taxpayer Services.
- (2) IRM 25.23.12.1.2(2) Updated Taxpayer Bill of Rights URL.
- (3) IRM 25.23.12.1.3 Updated title to Roles and Responsibilities.
- (4) IRM 25.23.12.1.4 Added new IRM section Program Management and Review.
- (5) IRM 25.23.12.1.5 Added new IRM section Program Controls.
- (6) IRM 25.23.12.1.6 Updated title to Terms and Acronyms. Removed ITAR from the Acronym listing.
- (7) IRM 25.23.12.2(2) Revised Reminder on how to perform authentication when TPP indicators are present.
- (8) IRM 25.23.12.2(2) Revised paragraph for dependent IP PIN inquires. Updated 1st & 2nd IF/THEN chart for dependent IP PIN inquires and to verify the identity of the parent or legal guardian using IDRS command code DDBKD under the dependent TIN to confirm the caller is the parent or legal guardian of the minor dependent. IPU 25U0364 issued 03-14-2025.
- (9) IRM 25.23.12.2(4) Updated chart for when the taxpayer calls in response to receiving a CP 01E.
- (10) IRM 25.23.12.2(5) Revised table row 1 to refer taxpayers to www.irs.gov/idtheft. Added new Reminder that advises the (Accounts Management Services) AMS IDT General Guidance checklist is available to assist with providing a complete list of identity theft guidance once the taxpayer has been authenticated and the account has been accessed.
- (11) IRM 25.23.12.3(2) Removed Exception that advised do not provide the caller with the opting-in via irs.gov option if their account has an unreversed TC 971 AC 527. IPU 25U0364 issued 03-14-2025.
- (12) IRM 25.23.12.3(2) Removed reference that advised callers they may receive correspondence acknowledging receipt of the Form 14039. Revised bullet to add IRS.gov.
- (13) IRM 25.23.12.4(2) Revised 2nd bullet to advise the Form 4566-F, Identity Theft Victims Request for Copy of Fraudulent Tax Return is available to complete and submit online through their Individual Online Account at IRS.gov/account under the Forms page.
- (14) IRM 25.23.12.4(7) Revised table rows to advise to electronically file with a current year return. Updated web page from www.irs.gov/getanippin to www.irs.gov/ippin. Revised sentence below chart as a new Reminder above chart.
- (15) IRM 25.23.12.4(7) Revised question in IF/THEN box #2 if the taxpayer does not know who claimed their dependent.

- (16) IRM 25.23.12.4(7) Revised question in IF/THEN box #2 to determine if the individual who claimed the dependent is a parent or legal guardian. Revised procedures when the response is yes by the taxpayer. IPU 25U3381 issued 06-06-2025.
- (17) IRM 25.23.12.4(7) Added REMINDER advising beginning in the 2025 filing season, the IRS will accept Forms 1040, 1040-NR and 1040-SS even if a dependent has already been claimed on a previously filed return as long as the primary taxpayer on the second return includes a valid Identity Protection Personal Identification Number (IP PIN). IPU 25U0471 issued 04-23-2025.
- (18) IRM 25.23.12.4(7) Added NOTE to IF/THEN box #1 and box #2 that advise tax returns claiming duplicate dependents for prior years (Tax Years 2023 and 2022) must still be filed by mail if the dependents have been claimed on another return. IPU 25U0364 issued 03-14-2025.
- (19) IRM 25.23.12.4(11) Revised timeframe from 493 days to 582 days. IPU 25U3381 issued 06-06-2025.
- (20) IRM 25.23.12.4(12) Removed reference to IRS.gov.
- (21) IRM 25.23.12.4.1(1) Added IDI2 as a tax-related identity theft case control. Removed IDI7 and IDI8 as a tax-related identity theft case control. IPU 25U0471 issued 04-23-2025.
- (22) IRM 25.23.12.4.1(3) Revised sentence for clarity.
- (23) IRM 25.23.12.4.1(4) Added new paragraph that advises to send a Letter 4445 if the taxpayer calls and states they never received their CP 01 acknowledgement letter.
- (24) IRM 25.23.12.4.1(6) Revised paragraph that advises to directly transfer balance due accounts in Status 22 to ACS.
- (25) IRM 25.23.12.4.1(9) Reworded note.
- (26) IRM 25.23.12.4.1(9) Revised timeframe from 493 days to 582 days. IPU 25U3381 issued 06-06-2025.
- (27) IRM 25.23.12.4.1(10) Added new NOTE that advises when the Form 14039 processing time frame has elapsed, and the Identity Theft claim remains unassigned, to reassign the case to a holding number. IPU 25U3381 issued 06-06-2025.
- (28) IRM 25.23.12.4.1(11) Added 4442 to sentence. IPU 25U0471 issued 04-23-2025.
- (29) IRM 25.23.12.4.4.1(5) Step 3 reworded for clarity.
- (30) IRM 25.23.12.4.9 Revised paragraph 6 and removed paragraphs 7 and 8 regarding research and refund trace procedures.
- (31) IRM 25.23.12.4.9 Deleted Receiving Calls on Accounts Involving IPSU Criteria; Identity Theft Assistance Request (ITAR) section. Subsequent IRMs renumbered. IPU 25U3381 issued 06-06-2025.
- (32) IRM 25.23.12.5(2) (3) Revised timeframe from 493 days to 582 days. IPU 25U3381 issued 06-06-2025.
- (33) IRM 25.23.12.5(2) Added guidance that Form 4506-F, Identity Theft Victims Request for Copy of Fraudulent Tax Return, can be submitted online through the taxpayer's Individual Online Account at IRS.gov/account.
- (34) IRM 25.23.12.6(1) Updated chart to advise of electronic option of submitting a Form 15227, Application for an Identity Protection Personal Identification Number (IP PIN).

- (35) IRM 25.23.12.6(1) Revised 2nd NOTE for taxpayers choosing to opt out of the IP PIN. IPU 25U0471 issued 04-23-2025.
- (36) IRM 25.23.12.6(1) Added to IF/THEN chart box 2 a taxpayer has two options to enroll for an IP PIN: Continuous Enrollment or One-Time Enrollment. IPU 25U0471 issued 04-23-2025.
- (37) IRM 25.23.12.6(1) For clarity, replaced the word **minor** with **Individuals under the age of 18**. IPU 25U0471 issued 04-23-2025.
- (38) IRM 25.23.12.6(1) Added new NOTE that advises once an opt-out selection is made, taxpayers will need to allow up to 72 hours before they are allowed to opt back in for an IP PIN. IPU 25U0364 issued 03-14-2025.
- (39) IRM 25.23.12.6(2) Revised note for clarity.
- (40) IRM 25.23.12.6(2) Revised CAUTION for clarity.
- (41) IRM 25.23.12.6(2) Removed bullet.
- (42) IRM 25.23.12.6(2) Revised sentence that advises employee's they **must** access and research the taxpayer's account if the taxpayer is calling regarding lost, misplaced or non-receipt of their or their dependent's annual IP PIN Notice CP 01A. IPU 25U3381 issued 06-06-2025.
- (43) IRM 25.23.12.6(2) Revised bullet for clarity. IPU 25U3381 issued 06-06-2025
- (44) IRM 25.23.12.6(2) Added CAUTION that IP PIN indicators should not be disclosed to spouses unless Third-Party Authentication has been met. Added the word Individual to the title for IRM reference IRM 21.2.1.62. IPU 25U0471 issued 04-23-2025
- (45) IRM 25.23.12.6(2) For clarity, replaced the word **minor** with **Individuals under the age of 18**. IPU 25U0471 issued 04-23-2025
- (46) IRM 25.23.12.6(2) Revised sentence that advises employees to perform authentication including additional authentication of the caller if it is required while using the IAT Disclosure Tool. IPU 25U0364 issued 03-14-2025
- (47) IRM 25.23.12.6(3) Added new paragraph to answer any general questions the caller may have related to the IP PIN program before accessing a taxpayer's account. IPU 25U3381 issued 06-06-2025
- (48) IRM 25.23.12.6.1(2) Revised bullet to advise to see www.irs.gov/ippin. Removed sentence that advised to call 800-829-3676. Updated bullets to advise of the <https://www.irs.gov/dmaf/form/f15227>.
- (49) IRM 25.23.12.6.1(2) (3) Revised timeframe from 493 days to 582 days. IPU 25U3381 issued 06-06-2025
- (50) IRM 25.23.12.6.1(7) Revised for clarity.
- (51) IRM 25.23.12.6.2(2) Reworded IF/Then box.
- (52) IRM 25.23.12.6.2(2) For clarity, replaced the word **minor** with **Individuals under the age of 18**. IPU 25U0471 issued 04-23-2025
- (53) IRM 25.23.12.6.3 Added the word Individual when referencing Individual Online Account. IPU 25U0471 issued 04-23-2025
- (54) IRM 25.23.12.7 Added new section Rescind – Form 14039 Identity Theft Affidavit.

- (55) IRM 25.23.12 Editorial changes have been made throughout the IRM for clarity. Reviewed and updated plain language, grammar, web addresses, IRM references, and legal references, where applicable. IPU 25U3381 issued 06-06-2025

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 25.23.12 dated 05-23-2025 and incorporates IMF Identity Theft Toll-Free Guidance IRM procedural updates: IPU 25U0364 issued 03-14-2025, IPU 25U0471 issued 04-23-2025, IPU 25U3381 issued 06-06-2025.

AUDIENCE

The provisions in the manual apply to all divisions, functional units, employees and contractors within the IRS performing Individual Master File (IMF) account/tax law work related to identity theft toll-free calls.

LuCinda Comegys
Director, Accounts Management
Taxpayer Services

25.23.12

IMF Identity Theft Toll-Free Guidance

Table of Contents

25.23.12.1 Program Scope and Objectives

25.23.12.1.1 Background

25.23.12.1.2 Authority

25.23.12.1.3 Roles and Responsibilities

25.23.12.1.4 Program Management and Review

25.23.12.1.5 Program Controls

25.23.12.1.6 Terms and Acronyms

25.23.12.1.7 Related Resources

25.23.12.2 Identity Theft Telephone General Guidance

25.23.12.2.1 Identity Theft Guidance for BMF Phone Calls

25.23.12.3 Non-Tax-Related Identity Theft - Self Identified

25.23.12.4 Tax-Related Identity Theft

25.23.12.4.1 Telephone Inquiries Regarding Identity Theft Victim Assistance (IDTVA) Tax-Related Cases

25.23.12.4.2 Open Identity Theft Victim Assistance (IDTVA) Controls - Call Back not Received by Taxpayer

25.23.12.4.3 Identity Theft - Freeze Codes

25.23.12.4.4 Identity Theft - Refund Inquiries

25.23.12.4.4.1 Identity Theft Cases from External Data Breaches

25.23.12.4.5 Identity Theft - Transcript Requests

25.23.12.4.5.1 Transcript NOT Requested - Taxpayer Claims Identity Theft

25.23.12.4.6 Identity Theft - Unpostables

25.23.12.4.7 Identity Theft - Balance Due Issues

25.23.12.4.8 Responses to IM Breach Notification Letter 4281C

25.23.12.4.9 Identity Theft - Economic Impact Payments (EIP)

25.23.12.5 Responses to Requests for copies of Fraudulent Return(s) for Identity Theft Victims

25.23.12.6 IP PIN Program Telephone Inquiries

25.23.12.6.1 Responding to Telephone Inquiries Regarding Form 15227 for Obtaining an IP PIN

25.23.12.6.2 Identity Protection Personal Identification Number (IP PIN) TAC Appointment Request
Received on Toll-Free Account Lines (App 20/21, 161/162)

25.23.12.6.3 Responding to Telephone Inquiries Regarding ID.me

25.23.12.7 Rescind – Form 14039 Identity Theft Affidavit

25.23.12.1
(10-01-2025)
Program Scope and Objectives

- (1) **Purpose:** This IRM provides Individual Master File (IMF) Identity Theft Toll-free victim assistance guidance and resource information.
- (2) **Audience:** This IRM is for use by all Taxpayer Service (TS) employees when responding to identity theft related telephone inquiries received on IRS toll-free numbers.
- (3) **Policy Owner:** The Director of Accounts Management.
- (4) **Program Owner:** Identity Protection Strategy and Oversight, Identity Theft Victim Assistance, Accounts Management, Taxpayer Services.
- (5) **Primary Stakeholders:** The following are primary stakeholders that Accounts Management collaborate with:
 - Return Integrity & Compliance Services (RICS)
 - Compliance
 - Submission Processing
- (6) **Program Goals:** Identity theft toll-free focuses on assistance activities and recommendations to help lighten the emotional and financial toll identity theft takes on its victims.
 - IRM 21.7.13, Assigning Employer Identification Numbers (EINs)
 - IRM 25.23.1, Identity Protection and Victim Assistance - Policy Guidance
 - IRM 25.23.2, Identity Protection and Victim Assistance - General Case Processing
 - IRM 25.23.3, IMF Non-Tax-Related IDT and Specialized Programs
 - IRM 25.23.4, IDTVA Paper Process
 - IRM 25.23.9, Business Master File (BMF) Identity Theft Processing
 - IRM 25.23.10, Compliance Identity Theft Case Processing

25.23.12.1.1
(10-01-2022)
Background

- (1) The Internal Revenue Service Commissioner's testimony before Congress on April 10, 2008 prompted Accounts Management (AM) to take a proactive position in combatting identity theft. A toll-free number for identity theft victims was created (800-908-4490). A caller residing outside the U.S. would call the International telephone number (267-941-1000). The procedures were created to assist taxpayers that are victims of tax-related identity theft and provide general guidance for non-tax related identity theft.

25.23.12.1.2
(10-01-2025)
Authority

- (1) Refer to IRM 1.1.13.7, Customer Account Services (CAS), for information.
- (2) The *Taxpayer Bill of Rights (TBOR)*, lists rights that already existed in the tax code, putting them in simple language and grouping them into 10 fundamental rights. Employees are responsible for being familiar with and acting in accord with taxpayer rights. See IRC 7803(a)(3), Execution of Duties in Accord with Taxpayer Rights. For additional information about the TBOR, see <http://www.irs.gov/tbor>.
- (3) Policy Statement 10-1, *Assisting Taxpayers who Report they are Victims of Identity Theft*. See IRM 1.2.1.17.1, P-10-1 (formerly P-25-1).

25.23.12.1.3
(10-01-2025)

Roles and Responsibilities

- (1) All taxpayers desire and expect courteous service. Taxpayers who experience identity theft are already victims, either emotionally or financially. All employees need to be aware of that impact and handle the contact with an additional level of sensitivity and understanding and be empathic when dealing with identity theft victims.
- (2) Additional information is found in IRM 1.1.13.7.3 , Accounts Management (AM), and IRM 21.1.1 , Accounts Management and Compliance Services Overview.
- (3) See IRM 21.1.1.1.3, Roles and Responsibilities, for Accounts Management, Compliance Services and Field Assistance employees.

25.23.12.1.4
(10-01-2025)

Program Management and Review

- (1) **Program Reports** - For reports concerning quality, inventory, aged listing, refer to IRM 1.4.16, Accounts Management Guide for Managers. Aged listings can also be reviewed by accessing Control Data Analysis, Project PCD. They are located on the Control-D/Web Access server, which has a login program control.
- (2) **Program Effectiveness** - Program Effectiveness is determined by Accounts Management's employees successfully using IRM guidelines to perform necessary account actions and duties effectively and efficiently.

25.23.12.1.5
(10-01-2025)

Program Controls

- (1) Goals, measures and operating guidelines are provided in the yearly Program Letter. Quality data and guidelines for measurement is referenced in IRM 21.10.1 , Embedded Quality (EQ) Program for Accounts Management, Campus Compliance, Field Assistance, Tax Exempt/Government Entities, Return Integrity and Compliance Services (RICS) and Electronic Products and Services Support.

25.23.12.1.6
(10-01-2025)

Terms and Acronyms

- (1) Refer to the table below for a list of acronyms used throughout this IRM.

Acronym	Definition
ACSS	Automated Collection System Support
AGI	Adjusted Gross Income
AMS	Account Management Services
APP	(phone) Application
ARP	American Rescue Plan
AUR	Automated Under Reporter
BFS	Bureau of the Fiscal Service
BMF	Business Master File
CAF	Centralized Authorization File
CDS	Centralized Distribution Site
CFOL	Corporate Files On-Line
CII	Correspondence Imaging Inventory
COB	Close of Business

Acronym	Definition
CSCO	Compliance Services Collection Operations
CSIRC	Computer Security Incident Response Center
CSR	Customer Service Representative
DV	Disclosure Verified
EFTPS	Electronic Federal Tax Payment System
EIP	Economic Impact Payment
EIP2	Second Economic Impact Payment
EIP3	Third Economic Impact Payment
EPSS	Electronic Products and Services Support
EUP	Employee User Portal
FAQ	Frequently Asked Questions
FTC	Federal Trade Commission
FRR	Fraudulent Return Request
GMP	Get My Payment tool
GRVW	Global Review
HRA IAT	High-Risk Authorization IAT
IAT	Integrated Automation Technologies
ICT	Image Control Team
IDRS	Integrated Data Retrieval System
IDT	Identity Theft
IDTVA	Identity Theft Victim Assistance
IM	Incident Management
IMF	Individual Master File
IPSO	Identity Protection Strategy and Oversight
IPSU	Identity Protection Specialized Unit (inventory process reference only, does not define teams/unit)
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology
ITIN	Individual Taxpayer Identification Number
MeF	Modernized e-File
MF	Master File

Acronym	Definition
OAR	Operations Assistance Request
P&A Analyst	Planning and Analysis Analyst
PII	Personally Identifiable Information
POA	Power of Attorney
RAIVS	Return and Income Verification Services
RPM	Return Preparer Misconduct
RRC	Recovery Rebate Credit
SBU	Sensitive But Unclassified
SERP	Servicewide Electronic Research Program
SP	Submission Processing
SSA	Social Security Administration
SSDI	Social Security Disability Benefits
SSI	Supplemental Security Income
SSN	Social Security Number
TAC	Taxpayer Assistance Center
TAS	Taxpayer Advocate Service
TDS	Transcript Delivery System
TE	Tax Examiner
TFA	Taxpayer First Act
TIN	Taxpayer Identification Number
TP	Taxpayer
TPP	Taxpayer Protection Program
TTG	<i>Telephone Transfer Guide</i>
USPS	United States Postal Service
VA	Veterans Affairs

25.23.12.1.7
(10-01-2023)

Related Resources

- (1) Various resources must be referred to and used as it relates to IDT Toll-free. Resources specific to IDT Toll-free are:

Note: The list of resources in the table below is not all inclusive as new resources are created and become available frequently.

Resource	Description
1. IAT Tools	There are various IAT tools created specific to IPSU inventory; IPSU IAT Tool. Refer to IRM 21.2.2.4.4.14, Integrated Automation Technologies, and Exhibit 21.2.2-2, Accounts Management Mandated IAT Tools.

Resource	Description
2. IRM 25.23	<p>Assistors should become acquainted with the list below of Identity Theft Victim Assistance (IDTVA) IRMs. This list is not all inclusive.</p> <ul style="list-style-type: none"> • IRM 25.23.1, Identity Protection and Victim Assistance - Policy Guidance • IRM 25.23.2, Identity Protection and Victim Assistance - General Case Processing • IRM 25.23.3, IMF Non-Tax-Related IDT and Specialized Programs • IRM 25.23.4, IDTVA Paper Process • IRM 25.23.9, Business Master File (BMF) Identity Theft Processing • IRM 25.23.10, Compliance Identity Theft Case Processing • IRM 25.23.11, Business Master File (BMF) Identity Theft Procedures for Accounts Management <p>Note: IRM 25.23.2, Identity Protection and Victim Assistance - General Case Processing, takes precedence over guidance presented in IRM 25.23.12, IMF Identity Theft Toll-Free Guidance, when processing and resolving identity theft claims. Closing actions are in 25.23.2, Identity Protection and Victim Assistance-General Case Processing.</p>
3. IRM 21	<p>Accounts Management (AM) IRMs - Utilize and become familiar with appropriate chapters. Refer to <i>SERP</i> for access to all IRM 21 chapters.</p>

Resource	Description
4. IDRS	Integrated Data Retrieval System (IDRS) This system is used for research and documenting taxpayer accounts as well as adjustment and closing actions for assigned cases.
5. SERP	Servicewide Electronic Research Program (SERP) Designed to provide employees with access to current IRMs, updated with interim procedural guidance, as well as reference materials. SERP provides employees with notification of IRM changes and current procedures.
6. AMS	Accounts Management System (AMS) This system is used for research and documenting taxpayer accounts as well as adjustment and closing actions for assigned cases.
7. EUP	Employee User Portal (EUP) This portal is used to access MeF for the Fraudulent Return Request (FRR).

25.23.12.2
(10-01-2025)
**Identity Theft Telephone
General Guidance**

- (1) Individuals may call the IRS to report their Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN) has been misused to obtain goods or services, to report other complaints of identity theft, and/or to request protection of their tax account information. An identity theft toll-free number 800-908-4490 (Application 161/162) is available specifically to receive identity theft related calls and provide taxpayer access to automated messages and assistants. The hours of operation are 7:00 a.m. to 7:00 p.m., Monday through Friday, (taxpayer's local time). Taxpayers calling from Alaska and Hawaii need to follow the Pacific Time. International callers would call 267-941-1000 (Non-toll free number) Monday through Friday, between the hours of 6:00 a.m. - 11:00 p.m. EST for all calls regarding identity theft. Refer to *Telephone Numbers (The Source)* for additional information on the telephone numbers provide and hours of operations.

Note: Calls should not be transferred to the identity theft toll-free number or application except for default screeners. Follow the *Telephone Transfer Guide* to determine when the transfer of a call is appropriate.

- (2) Accounts Management Customer Service Representatives are required to use the IAT Disclosure tool to perform required and additional taxpayer authentication.

tion when the IRM requires it. See Exhibit 21.2.2-2, Accounts Management Mandated IAT Tools. Additional authentication must be completed when the IAT Disclosure tool alerts the users to account conditions when identity theft is suspected, a factor, or documented. This includes accounts involving multiple entities, mixed periods, an MFT 32 account, cases involving IDT related transactions, open identity theft controls, etc. A list of identity theft action codes can be found in IRM 25.23.2, Identity Protection and Victim Assistance - General Case Processing.

Reminder: Calls with Taxpayer Protection Program (TPP) involvement received by non TPP CSRs require basic taxpayer authentication. Additional authentication will be required when there are other account conditions, such as an open or unresolved identity theft marker.

See IRM 25.25.6.6, Non Taxpayer Protection Program Telephone Assistors Response to Taxpayers, when the call meets TPP criteria to see if additional authentication is required. If required, authentication procedures should be completed prior to taking any actions on the account.

The following are additional references which discuss disclosure.

- IRM 21.1.1.4, Communication Skills
- IRM 21.1.3.2.3, Required Taxpayer Authentication
- IRM 21.1.3.2.4, Additional Taxpayer Authentication
- IRM 21.1.3.3, Third Party (POA/TIA/F706) Authentication
- IRM 21.1.3.20.1, IMF and BMF Oral Statement Address Changes
- IRM 21.6.2.3.3, Telephone Inquiries Regarding Mixed Entity and Scrambled SSN Cases
- *TCD 0249, Communication Skills*
- IRM 11.3.2, Disclosure to Persons with a Material Interest
- Pub 17, Your Federal Income Tax (For Individuals), Part One, Chapter Three, Dependents, for situations where a taxpayer may be eligible to authenticate on behalf of their dependent qualifying child.

There will be times when you receive a call from a parent, legal guardian, or other individual who reports the identity theft, or wants to inquire about an IP PIN of a minor dependent (under the age of 18). If you receive a call from an individual inquiring about another individual's Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN) that was used fraudulently on a tax return, or wants to inquire about an IP PIN then follow the chart below:

Caution: Parents or legal guardians of adult dependents should be treated as a third party contact

If	And	Then
<p>1. You receive a call from a parent/legal guardian of a minor dependent (under the age of 18) regarding an open or closed identity theft claim under the dependent's TIN,</p> <p>or</p> <p>wants to inquire about an IP PIN,</p> <p>or</p> <p>there's allegations from the parent/legal guardian for a rejected e-filing message</p>	<p>There is a Masterfile account established for the dependent's TIN</p>	<p>Conduct Required Taxpayer Authentication and Additional Taxpayer Authentication on the parent/legal guardian using their TIN and conduct Required Taxpayer Authentication with the parent/legal guardian, on the dependent.</p> <p>Verify the identity of the parent or legal guardian using IDRS command code DDBKD under the dependent TIN to confirm the caller is the parent or legal guardian of the minor dependent</p> <p>Notate AMS with detailed history:</p> <ul style="list-style-type: none"> • Under parent/legal guardian's TIN indicate pass/fail and dependent's TIN, name and date of birth. • Under dependent's TIN indicate parent's name and TIN used for authentication.

If	And	Then
<p>2. You receive a call from a parent/legal guardian of a minor dependent (under the age of 18) calling regarding an open or closed identity theft claim under the dependent's TIN,</p> <p>or</p> <p>wants to inquire about an IP PIN,</p> <p>or</p> <p>there's allegations from the parent/legal guardian for a rejected e-filing message</p>	<p>There is no Masterfile account established for the dependent's TIN</p>	<p>Conduct Required Taxpayer Authentication and Additional Taxpayer Authentication on the parent/legal guardian using their TIN and verify the TIN, Name, and DOB of the dependent.</p> <p>Verify the identity of the parent or legal guardian using IDRS command code DDBKD under the dependent TIN to confirm the caller is the parent or legal guardian of the minor dependent</p> <p>Notate AMS with detailed history:</p> <ul style="list-style-type: none"> • Under parent/legal guardian's TIN indicate pass/fail and dependents TIN, name and date of birth. • Under dependent's TIN indicate parent's name and TIN used for authentication.

If	And	Then
<p>3. You receive a call from a parent or legal guardian of a dependent who is no longer a minor (Age 18 or older)</p> <p>or</p> <p>You receive a call from an individual who is not a parent or legal guardian of a minor or an individual requesting information on another individual's account who is age 18 or older</p>		<p>Continue to IRM 21.1.3.3, Third-Party (POA/TIA/F706) Authentication, for third-party authorization requirement. You must not disclose any information until you are certain that the person with whom you are speaking is an authorized third-party.</p> <p>Notate AMS with detailed history:</p> <ul style="list-style-type: none"> • Under the minor or individuals TIN indicate the third party individual whom you spoke with and indicate pass/fail.

- (3) Guidance will be provided to individuals identifying themselves or their dependent as potential victims of identity theft, including actions to take when there is currently no tax-related impact or tax-related identity theft. It is important to identify the issue and/or the reason the taxpayer is calling (IP PIN issue, balance due notice, refund offset, rejected e-file, lost or stolen purse/wallet, etc.) and follow those IRM guidelines.
- (4) Some identity theft issues (TPP, data breaches, EIN issues, Preparer Misconduct, Unemployment IDT), require further research. See the If/Then chart below:

If	Then
Your research determines the taxpayer's inquiry received on the toll-free lines (examples: App 20/21 or 161/162) meets Taxpayer Protection Program (TPP) criteria,	Follow procedures in IRM 25.25.6.6, Non Taxpayer Protection Program (TPP) Telephone Assistors Response to Taxpayers.
The call is from an individual who claims they received an Employer Identification Number (EIN) but did not apply for one or does not own a business,	See IRM 25.23.12.2.1, Identity Theft Guidance For BMF Phone Calls.

If	Then
The call is from a business entity that has experienced a data breach,	Refer to IRM 25.23.1.6, Data Breach - Business Entities Whose Employees or Clients PII was Breached, for instructions.
The call is from an individual who is a victim of an external data breach,	Refer to IRM 25.23.1.7, Taxpayers who are Victims of a Data Breach, for instructions.
The call is from an individual alleging Return Preparer Misconduct (RPM) rather than identity theft,	Refer to IRM 25.24.1.3, Identifying Potential RPM Issues for Telephone Assistors/Taxpayer Assistance Center (TAC) Assistors.

If	Then
<p>The call is from a taxpayer reporting that they are a victim of Unemployment Identity Theft (also known as Unemployment Compensation, Insurance, or Benefits),</p>	<ol style="list-style-type: none"> 1. Advise the taxpayer they may want to contact the state Department of Labor (DOL) where the Unemployment Identity Theft occurred. The DOL agency will assist them. Provide the Agencies web addresses, and contact numbers below: <ul style="list-style-type: none"> • U.S. Department of Labor (DOL) Reporting Unemployment Identity Theft: https://www.dol.gov/fraud and, https://www.dol.gov/agencies/eta/UIIDtheft#state-directory for information on individual states unemployment agency reporting identity theft claims. <p>Contact Number: 1-866-487-2365</p> 2. For Unemployment Identity Theft during the COVID-19 pandemic contact the <i>U.S. Department of Justice National Center for Disaster Fraud (NCDF)</i>. <ul style="list-style-type: none"> • National Center for Disaster Fund Complaint Form https://www.justice.gov/disaster-fraud/ncdf-disaster-complaint-form <p>Contact Number: 1-866-720-5721</p>
<p>The call is in response to the taxpayer receiving a CP 01E</p>	<p>See IRM 25.23.2.8.5(9), Employment-related Identity Theft – TC 971 AC 525 for additional guidance.</p>

- (5) Once you have determined the issue and performed the necessary authentication, ask if the taxpayer would prefer to receive identity theft information via the internet or over the phone.

Reminder: The (Accounts Management Services) AMS IDT General Guidance checklist is available to assist with providing a complete list of identity theft guidance once the taxpayer has been authenticated and the account has been accessed.

If	Then
1. Taxpayer prefers to access via the internet	1. Provide the IRS website, www.irs.gov/idtheft .

If	Then
<p>2. Taxpayer states internet access is not an option, or they prefer to receive the resource information over the phone</p>	<p>Provide the following recommendations as applicable:</p> <ol style="list-style-type: none"> 1. Advise the taxpayer they must continue to file their tax returns and pay the taxes as appropriate while their identity theft claim is under review. 2. Advise the taxpayer they should contact their financial institution to report the allegation of identity theft. 3. Advise the taxpayer to check their local state agencies to determine if additional steps are required at the state level. 4. Advise the taxpayer there may be a few situations where they would also file a report with their local or state police. (i.e., If they know the identity thief or have other information that could help a police investigation, Or if the identity thief used their name during a traffic stop, any encounter with the police, or, if a creditor, debt collector, or someone else affected by the identity theft insists the victim provide a police report). 5. Advise the taxpayer to contact one of the three major credit bureaus listed below and provide the web address and contact phone number. They will assist them in identifying what specific information is needed to pursue an allegation of identity theft. <ul style="list-style-type: none"> • Equifax www.equifax.com 800-525-6285 • Experian www.experian.com 888-397-3742 • TransUnion www.transunion.com 800-680-7289 6. Advise the taxpayer they may contact the two agencies listed below if they are concerned about protecting their identity (including their SSN) to prevent misuse. Provide the web address and contact phone number. The agencies will assist them in identifying what specific information is needed to pursue an allegation of identity theft. <ul style="list-style-type: none"> • Federal Trade Commission (FTC) www.identitytheft.gov 877-438-4338 <p>Note: For victims needing to complete Form 14039, the IRS is currently providing an on-line <i>Form 14039</i> at https://www.irs.gov/dmaf/form/f14039. This is in addition to the fillable FTC Form 14039 available at identitytheft.gov. This is authorized by the IRS and its present placement on the FTC site is intended as providing an additional resource for identity theft victims who are self-reporting to the FTC. The victim should only file one Form 14039, either directly with the IRS or through the FTC. CSR's should not attempt to provide assistance with the functionality of the FTC website. See IRM 25.23.2.2.1, Taxpayer Interaction.</p> <ul style="list-style-type: none"> • Social Security Administration (SSA) www.ssa.gov (type in identity theft in the search box) 800-772-1213

If	Then
	<p>7. Advise the taxpayer Publication 5027, Identity Theft Information for Taxpayers, provides the above resource information in English, Spanish, and Braille. This publication and other publications can be obtained electronically on the IRS website, www.irs.gov.</p> <p>Note: There are numerous websites and publications available to the public to assist with the prevention of becoming a victim of identity theft and with steps on how to protect personal identifying information (PII) etc. The recommendations above are not all inclusive. If the caller mentions or questions other websites or publications, simply provide a word of caution to ensure the website they are referencing is legitimate.</p> <p>8. Provide the caller with the identity theft toll-free number including the hours of operation located in paragraph (1) above when appropriate.</p>

- (6) If the taxpayer asks for information about the investigation or prosecution of an identity thief, tell them the U.S. Department of Justice prosecutes cases of identity theft and fraud under a variety of federal statutes. Federal prosecutors work with federal investigative agencies such as the Federal Bureau of Investigation (FBI), the United States Secret Service, and the United States Postal Inspection Service to prosecute identity theft and fraud cases. Schemes to commit identity theft or fraud may involve violations such as identification fraud, credit card fraud, computer fraud, mail fraud, wire fraud, or financial institution fraud. Each of these federal offenses are felonies that carry substantial penalties and, in some cases, as high as 30 years' imprisonment, fines, and criminal forfeiture. If the taxpayer would like additional information, refer them to www.justice.gov. Advise the taxpayer to search using the key words "identity theft".
- (7) Each situation needs to be researched to determine if there is an impact to the taxpayer's account. Refer to If/And/Then chart below:

Note: See Exhibit 25.23.1-1, Glossary of Identity Protection Terms and Definitions, and IRM 25.23.2.4.1, Tracking and Reporting Identity Theft Cases - Identity Theft Indicators, to assist with your determination.

If the Caller's inquiry is about	And	Then
Non-Tax-Related	Self-identified identity theft issues	Refer to IRM 25.23.12.3, Non-Tax Related Identity Theft - Self Identified
Tax-related	Identity Theft	Refer to IRM 25.23.12.4, Tax Related Identity Theft

If the Caller's inquiry is about	And	Then
Dependent	Identity Theft	<p>Refer to IRM 25.23.2.3.1, Dependent Identity Theft</p> <p>Refer to IRM 25.23.12.4, Tax Related Identity Theft for additional Dependent Identity Theft guidance.</p> <p>Note: If during a call your research determines there is an open identity theft case, refer to IRM 25.23.4.8.4, Dependent Related Identity Theft (IDT) - General.</p>
IP PIN Program	<ul style="list-style-type: none"> • Ways to Enroll • Status of application (Form 15227, Application for an Identity Protection Personal Identification Number (IP PIN)) • Non-Receipt, lost, or misplaced • Opting out of IP PIN 	Refer to IRM 25.23.12.6, IP PIN Program Telephone Inquiries
Transcripts	Identity Theft	Refer to IRM 21.2.3.5.8, Transcripts and Identity Theft for Individuals.

25.23.12.2.1
(06-21-2024)

**Identity Theft Guidance
for BMF Phone Calls**

- (1) Complete all initial research to rule out normal account issues and determine if the potential for ID theft exists.
- (2) In many instances, a third party requested an EIN on the taxpayer's behalf for a legitimate business purpose. When the caller indicates no knowledge of the EIN or business account, expand the normal probe questions to include:
 - Did a family member take over a previously owned business and request an EIN in your name or continue to use an inactive EIN assigned to you several years ago?
 - Did you join a partnership or participate in the creation of a company where you provided your taxpayer identification number (TIN)?
 - Did you provide your TIN to a community association or accountant to prepare tax returns on your behalf or a third party?
 - Did you create a trust or other fiscal entity through a bank or executor?
 - Have you received any home care services while enrolled in a program administered by a Federal, state, or local government agency that provides funding for the home care services? If yes, a 3rd party Agent may be authorized to act on behalf of the home care recipient to report and pay Federal employment taxes which requires an EIN.

Note: This list is not all inclusive and additional probes can be found at IRM 25.23.9.4(3), BMF Identity Theft Research.

- (3) Based on the taxpayer answers to the questions in (2) above, follow the table below.

IF	THEN
1. The taxpayer answers yes to any of the questions in (2) above	Notify the taxpayer they are not a victim of identity theft. If the taxpayer wants to protect themselves from identity theft, follow normal guidance in the IRM 25.23.12.2, Identity Theft Telephone General Guidance.
2. The taxpayers answers no to all the questions in (2) above	Refer to IRM 25.23.2.4.3, Tracking Individual Taxpayers Reporting to be Victims of Business-Related Identity Theft. Research the taxpayer's TIN to determine if there are any actions required on the taxpayer's IMF account prior to completing a Form 14566, BMF Identity Theft Referral.

25.23.12.3
(10-01-2025)
**Non-Tax-Related Identity
Theft - Self Identified**

- (1) Individuals experiencing non-tax-related identity theft may call the IRS for guidance (lost or stolen wallet, fraudulent unemployment claims, etc). Review and research of the taxpayer's account is **not** necessary if non-tax related identity theft guidance is the **only** issue the taxpayer is experiencing. It is important to identify the issue and/or the reason the taxpayer is calling (IP PIN issue, balance due notice, refund offset, rejected e-file, other open issues, etc.) and follow those IRM guidelines.

Note: If the taxpayer is inquiring about phishing and other scams, refer to IRM 21.1.3.23, Scams (Phishing) and Fraudulent Schemes.

- (2) Take the following actions:

- a. Provide guidance and resource information as referenced in IRM 25.23.2, Identity Protection and Victim Assistance - General Case Processing, and IRM 25.23.2.3.6, When to Request Additional Information to Support an Allegation of Identity Theft.
- b. Advise the caller the best way to protect their TIN (SSN/ITIN) is by participating in the IP PIN Program. Opting-in or applying to participate helps prevent the misuse of their Social Security number on any future federal income tax returns filed. An IP PIN helps the IRS verify a taxpayer's identity and accept their electronic or paper returns. See IRM 25.23.12.6, IP PIN Program Telephone Inquiries, for a list of options available for individuals to enroll in the program.
Provide the caller with information on opting-in or applying to participate in the IP PIN Program.
- c. Advise participating in the IP PIN Program is voluntary for taxpayers who are not victims of tax-related identity theft. To find out if a taxpayer is eligible to opt-out, they would need to log into their Individual Online Account.
- d. Advise the taxpayer it is unnecessary to file Form 14039, Identity Theft Affidavit, for a non-tax related issues if the taxpayer opts-in to the IP PIN program.
If the caller insists or states they will submit Form 14039, then advise callers they may receive correspondence requesting additional information.
If the caller request guidance for submitting the form either through the FTC website, IRS.gov, or by paper refer to IRM 25.23.2.3, Identity Theft Claims - General Guidelines, and IRM 25.23.2.2.1, Taxpayer Interaction.
Advise the taxpayer that once their form is processed, they will receive a notice providing them the option again to participate in IP PIN Program.

Note: See IRM 25.23.12.6, IP PIN Program Telephone Inquiries, for a list of options available for individuals to enroll in the program.

- e. Advise the caller to use the identity theft toll-free number (800-908-4490) for all subsequent calls regarding non-tax-related identity theft. The hours of operation are 7:00 a.m. - 7:00 p.m. Monday - Friday. Taxpayers calling from Alaska and Hawaii adhere to Pacific Time frames. International caller would call 267-941-1000 (not toll-free) Monday through Friday, between the hours of 6:00 a.m. - 11:00 p.m. EST for all subsequent calls regarding non-tax related identity theft.

25.23.12.4
(10-01-2025)
Tax-Related Identity Theft

- (1) When taxpayers call to report tax-related identity theft, probe the taxpayer to determine if they received a notice or a bill related to unknown income, or received notification of an audit. Review and research the taxpayer's account to determine if additional information is needed. Refer to IRM 25.23.2.3, Identity Protection and Victim Assistance - General Guidelines, and IRM 25.23.2.3.6, When to Request Additional Information to Support an Allegation of Identity Theft, for guidance on when a taxpayer should submit a claim and when additional information is needed. See Exhibit 25.23.1-1, Glossary of Identity Protection Terms and Definitions, for the definition of an "Identity Theft Claim".

Note: If compliance is involved with the case, Form 14039 must be submitted with the taxpayers' response.

Exception: For taxpayer inquiries received on the toll-free lines (examples: App 20/21 or 161/162) that meet Taxpayer Protection Program (TPP) criteria (i.e., taxpayer states they received one of the following letters addressed to them, Letter 4883C, Letter 5071C, Letter 5447C or Letter 5747C; or there is an Unpostable 126 RC 0), see IRM 25.25.6.6, Non Taxpayer Protection Program (TPP) Telephone Assistors Response to Taxpayers.

Note: If during your research you find an open identity theft case control such as an IDT(x), IDS(x), (the "x" represents an IDT/S 1, 3, 6, 7, 8, or 9) **or** IDI(x) (the "x" represents an IDI 1, 2, 3, 4, 5, 6, or 9), see IRM 25.23.12.4.1, Telephone Inquiries Regarding Tax-Related Identity Theft Victim Assistance (IDTVA) Cases, for additional information and guidance.

Caution: **Do not** advise the caller to complete a Form 3949-A, Information Referral, if the caller has identity theft involving misuse of their own TIN (SSN/ITIN), they have a problem related to their own tax return and tax return preparer, or they received a Duplicate TIN soft notice and want to provide information on the other taxpayer claiming the exemption or Earned Income Tax Credit. See IRM 21.1.3.19, Informant Contacts.

Note: If a taxpayer is calling to report the theft of their refund (ex: stolen from their mailbox, mailed to an incorrect address, stolen from their wallet) or, if their refund was deposited to an incorrect account or closed account, refer to IRM 21.4.2, Refund Trace and Limited Payability.

- (2) Be empathetic to the taxpayer's issue. Assure the taxpayer that the IRS is committed to working with them to resolve their identity theft issues. Cases such as theirs require complete and thorough research to provide them with a status update and to make a correct determination for case resolution.
- (3) If the taxpayer's call is regarding their Economic Impact Payment (EIP) and they are claiming to be a victim of identity theft, see IRM 25.23.12.4.9, Identity Theft - Economic Impact Payments.
- (4) If the taxpayer calls regarding an Identity Protection Personal Identification Number (IP PIN) issue such as lost, misplaced, non-receipt, or electronic filing rejection even though they used their IP PIN, refer to IRM 25.23.12.6, IP PIN Program Telephone Inquiries, for guidance on assisting the taxpayer.
- (5) If the taxpayer is calling for the status of their Form 4506-F, Request for Copy of Fraudulent Tax Return and there is an open IDT7 on the account, refer to

IRM 25.23.12.5, Responses to Requests for copies of Fraudulent Return(s) for Identity Theft Victims.

- (6) If the taxpayer received a reject message after attempting to e-file due to the primary and/or secondary TIN(s) having already been used to e-file a return, then advise the taxpayer to file a paper return with a Form 14039, Identity Theft Affidavit, attached. Advise the taxpayer a fillable Form 14039 is available on IRS.gov. Enter AMS narrative by selecting **Identity Theft; "TP will file paper return with IDT claim"**.
- (7) If the taxpayer is contacting IRS about receiving a rejection message after attempting to e-file for a dependent's TIN, follow procedures in IRM 25.23.12.2(2), Identity Theft Telephone General Guidance, If and Then Chart to authenticate the taxpayer and minor dependent. Ask the taxpayer to confirm the TIN submitted electronically for the dependent matches the information on their social security card or ITIN assignment letter.

Reminder: Beginning in the 2025 filing season, the IRS will accept e-filed Forms 1040, 1040-NR and 1040-SS even if a dependent has already been claimed on a previously filed return as long as the primary taxpayer on the second return includes a valid Identity Protection Personal Identification Number (IP PIN). This change will reduce the time for the agency to receive the tax return and accelerate the issuance of tax refunds for those with duplicate dependent returns. In previous years, the second tax return had to be filed by paper.

Reminder: For general information on Dependent Related Identity Theft (IDT), refer to IRM 25.23.4.8.4, Dependent Related Identity Theft (IDT) - General and IRM 25.23.2.3.1, Dependent Identity Theft.

If research confirms	Then
<p>1. TIN matches and the dependent's TIN is being used as a primary or secondary TIN on another tax return</p> <p>Reminder: Do not disclose information on the return filed under the dependent's TIN.</p>	<ol style="list-style-type: none"> 1. Advise the taxpayer that to electronically file a current year return with this dependent, the taxpayer will be required to use an Identity Protection Personal Identification Number (IP PIN). Direct them to www.irs.gov/ippin for information on the IP PIN and how to obtain one. Advise the taxpayer that if they are unable to get an IP PIN or do not wish to get an IP PIN, then they would need to file a paper return. Note: Tax returns claiming duplicate dependents for prior years (Tax Years 2023 and 2022) must still be filed by mail if the dependents have been claimed on another return. 2. Advise a Form 14039 can be submitted separately for/by the dependent whose TIN was used fraudulently. For victims needing to complete Form 14039, the IRS is currently providing an on-line <i>Form 14039</i> at https://www.irs.gov/dmaf/form/f14039 on <i>IRS.gov</i>. 3. Enter AMS and select Identity Theft, then enter narrative "TP will file paper return and advised the dependent should file Form 14039 IDT claim." 4. If a dependent's TIN is being used on another return fraudulently and taxpayer will file Form 14039, follow the procedures in IRM 25.23.2.4.4, Initial Allegation or Suspicion of Tax-Related Identity Theft - IMF Identity Theft Indicators, for the input of TC 971 AC 522. 5. Continue with the call following procedures in paragraph 9 below.

If research confirms	Then
<p>2. The dependent's TIN is being used as a dependent on another tax return and they received a reject message after attempting to e-file.</p> <p>Reminder: Do not disclose information on the return the dependent was claimed on.</p>	<ol style="list-style-type: none"> 1. Advise the taxpayer that to electronically file a current year return with this dependent, the taxpayer will be required to use an Identity Protection Personal Identification Number (IP PIN). Direct them to www.irs.gov/ippin for information on the IP PIN and how to obtain one. Advise the taxpayer that if they are unable to get an IP PIN or do not wish to get an IP PIN, then they would need to file a paper return. <p>Note: Tax returns claiming duplicate dependents for prior years (Tax Years 2023 and 2022) must still be filed by mail if the dependents have been claimed on another return.</p> 2. Is the individual who claimed the dependent a parent or legal guardian? <ul style="list-style-type: none"> • If the answer is no, or the taxpayer does not know who claimed their dependent advise the taxpayer a Form 14039 can be submitted separately for/by the dependent whose TIN was used fraudulently. For victims needing to complete Form 14039, the IRS is currently providing an on-line <i>Form 14039</i> at https://www.irs.gov/dmaf/form/f14039 on <i>IRS.gov</i>. Enter AMS and select Identity Theft, then enter narrative "TP will file paper return and advised the dependent should file Form 14039 IDT claim." • If the answer is yes, and it is the parent or legal Guardian, then it is not considered dependent identity theft. Provide the caller with options available for the dependent to protect their TIN by filing a Form 15227, Application for an Identity Protection Personal Identification Number (IP PIN). Enter AMS, input a narrative "TP was advised of options available to protect dependent's TIN." <p>Reminder: IDTVA employees are not making a determination regarding which parent/legal guardian is entitled to claim and/or represent the dependent.</p> 3. Advise a Form 14039 can be submitted separately for/by the dependent whose TIN was used fraudulently. 4. Follow procedures in IRM 25.23.2.4.4, Initial Allegation or Suspicion of Tax-Related Identity Theft - IMF Identity Theft Indicators, for inputting a TC 971 AC 522 if the taxpayer states they will be filing a Form 14039. If there is no established entity and you receive a response of "No Account on TIF" then enter these additional case notes on AMS when selecting Identity Theft in (2) above: "No established account on TIF - TP PND-CLM DEP IDT".

If research confirms	Then
	5. Continue with the call following procedures in paragraph 9 below.

- (8) If the taxpayer is responding to an IRS letter or notice (with the exception of the TPP letters referenced above), advise the taxpayer to submit an identity theft claim, when appropriate, with a copy of the IRS letter or notice. Send the information to the address indicated on the letter or notice. Enter AMS narrative by selecting **Identity Theft, "TP will respond to letter/notice with IDT claim."**

Reminder: Advise the taxpayer to include any additional information such as written statements, supporting evidence, credit bureau letters etc. the notice/letter is requesting (example: an AUR notice may include a request that all income issues be addressed and whether they are part of the identity theft impact).

Reminder: If the taxpayers call about an IRS balance due issue on a new identity theft claim refer to IRM 25.23.12.4.7, Identity Theft – Balance Due Issues, and IRM 5.19.21.2.1, Identity Theft Claim.

- (9) Advise the taxpayer there will be processing delays while the situation is resolved and they may receive correspondence requesting additional information.
- (10) Provide taxpayers with a realistic expectation of the time frame for resolution of their cases. Explain that identity theft is complex in nature and constantly changing. Apologize to the taxpayer for the length of time required to resolve their issue. Suggested language is:
I apologize for the length of time it is taking to resolve your case. Identity theft is a challenging and ever-changing issue, and we are working with victims like you to resolve tax-related identity theft cases. We take identity theft seriously and are committed to resolving identity theft cases as quickly as possible and are taking steps to reduce this timeframe. You will receive notification once your case has been resolved.
- (11) Advise that most cases are resolved in 120 days or less but due to extenuating circumstances caused by the pandemic our identity theft inventories have increased dramatically. On average it is taking us 582 days to resolve identity theft cases. Explain that identity theft cases are worked in the order they are received. If the taxpayer has further questions on the timeframe, advise the taxpayer to visit the IRS.gov web address and type "Processing Status" in the search bar to check the current operational status.
- (12) Individuals not required to file a return may also be negatively impacted by tax-related identity theft. For example, a taxpayer may state the Social Security Administration (SSA) has reduced or stopped their Social Security benefits based on a tax return filed with the IRS. The taxpayer indicates that they have not filed a return. When this type of call is received, follow the instructions below:
- Advise the taxpayers to submit a claim using the on-line Form 14039, currently available on at <https://www.irs.gov/dmat/form/f14039> on *IRS.gov*. Include an explanation of their situation. If the taxpayer has any

additional information they may think would be appropriate to substantiate their situation, provide the taxpayer with the alternative option of either mailing or faxing their claim. If taxpayer chooses to fax their claim, advise them to follow the faxing instructions provided on the second page of Form 14039. Enter AMS narrative and select Identity Theft; **“NFR - TP will respond to letter/notice with IDT claim.”** If a taxpayer is not required to file a return and chooses to mail their claim, they will need to submit their Form 14039 to: Department of the Treasury Internal Revenue Service Fresno, CA 93888-0025

- Advise the taxpayer they may receive correspondence requesting additional information.

Note: If the taxpayer states they are experiencing an economic hardship because of this event, refer to IRM 21.1.3.18, Taxpayer Advocate Service (TAS) Guidelines.

- (13) Input a TC 971 AC 522 per IRM 25.23.2.4.4, Initial Allegation or Suspicion of Tax-Related Identity Theft - IMF Identity Theft Indicators, and Exhibit 25.23.2-10, IMF Only TC 971 AC 522 Tax-Related Identity Theft, Case Status (Initial Claim/Suspicion).

25.23.12.4.1
(10-01-2025)
**Telephone Inquiries
Regarding Identity Theft
Victim Assistance
(IDTVA)Tax-Related
Cases**

- (1) A tax-related identity theft case controlled on IDRS can be identified by control categories, IDT(x), IDS(x) (the “x” represents an IDT/S 1, 3, 6, 8, or 9), **or** IDI(x) (the “x” represents an IDI 1, 2, 3, 4, 5, 6, or 9). A telephone CSR **must not** adjust or take any account actions on these **open** identity theft accounts except when the account meets Taxpayer Protection Program (TPP) criteria. Refer to IRM 25.25.6.6, Non Taxpayer Protection Program (TPP) Telephone Assistors Response to Taxpayers.
- (2) Accounts Management Customer Service Representatives are required to use the IAT Disclosure tool to perform required and additional taxpayer authentication when the IRM requires it. See Exhibit 21.2.2-2, Accounts Management Mandated IAT Tools. Additional authentication must be completed when the IAT Disclosure tool alerts the users to account conditions when identity theft is suspected, a factor, or documented. This includes accounts involving multiple entities, mixed periods, an MFT 32 account, or cases involving IDT related transactions, open identity theft controls, etc.
A list of identity theft action codes can be found in IRM 25.23.2, Identity Protection and Victim Assistance - General Case Processing. Refer to IRM 21.1.3.2.3, Required Taxpayer Authentication, and IRM 10.10.3.3.7, Identity Proofing for Additional Taxpayer Authentication, for high-risk authentication procedures. If IAT Disclosure tool is not available or an employee has a problem with the IAT Tool Manager, the case should be processed through IDRS following established procedures. See IRM 21.2.2.4.4.14 (2), Integrated Automation Technologies, for additional information.
- (3) If the identity theft case is **closed or resolved**, you may provide account information to the TIN owner after authenticating them. You may provide the TIN owner with the information from their account only. There may be fraudulent information combined with the TIN owner’s information, such as IRP data, account transcripts, etc. Do not provide information from the fraudulent return. If the taxpayer is asking for their own transcript information, see IRM 21.2.3.5.8, Transcripts and Identity Theft. Also refer to IRM 21.2.3.5.8.4.3, Wage and Income Transcript Identity Theft, and IRM 25.23.2.10, Get Transcript

25.23 Identity Protection and Victim Assistance

Breach. You can usually identify the following transaction(s) on Integrated Data Retrieval System (IDRS) via cc ENMOD and/or cc IMFOLE, if the case is resolved.

- A posted TC 971 AC 501 or
- A posted TC 971 AC 506

See IRM 25.23.2.4.1, Tracking and Reporting Identity Theft Cases - Identity Theft Indicators, for additional information related to IDT indicators.

Note: Accounts or cross-reference accounts with TC 971 AC 501, 506, 522, 524 or 525 will not be able to receive transcripts via online, mail order or phone services. Taxpayers are instructed to contact the IDT toll free number for the transcript. Do not refer the taxpayer to self-serve options. See IRM 21.2.3.5.8, Transcripts and Identity Theft, for additional guidance. For guidelines on issuing a specific type of transcript see IRM 21.2.3.5.8.4, Type of Transcript Requested for Identity Theft Accounts.

#

Note: Because there may be instances where an AC 501 or AC 506 is prematurely placed on an account, careful and complete research must be conducted to ensure all actions to resolve the identity theft issue are taken. (EX: CP 01, Letter 4674C, or Letter 239C has been issued to the taxpayer.)

- (4) A CP 01, Identity Theft Claim Acknowledgement is used to acknowledge receipt of a Form 14039 substantiating a claim of identity theft and to notify taxpayers of the action taken by the IRS with regard to their tax records. This notice is issued systemically after the TC 971 AC 501 is input on the taxpayer's account. If the taxpayer calls stating they never received this notice, research CC ENMOD and IMFOLE to confirm the notice was issued. If the notice was issued, a Letter 4445C, ID Theft Acknowledgement Notification, can be sent.
- (5) For a closed identity theft case, if the **SSN owner** did not receive their refund, received an incorrect refund amount, or received an incorrect balance due notice because the case is worked incorrectly, (for example, an employee failed to input the TC 971 AC 850 causing a direct deposit into the bad taxpayer's account), treat the case as priority work and take the following actions:

If the case	Then
1. Can be resolved over the telephone, see IRM 21.1.3.20, Oral Statement Authority, and IRM 21.5.2.4.2, Adjustments with Oral Statement	Input the adjustment.
2. Cannot be resolved over the phone and the case meets: <ul style="list-style-type: none"> • TAS criteria, see IRM 13.1.7.3.1, TAS Case Criteria 1-4, Economic Burden 	Complete the correct referral to TAS following guidance in IRM 21.1.3.18, Taxpayer Advocate Service (TAS) Guidelines.

If the case	Then
3. Cannot be resolved over the telephone and case does not meet TAS Criteria 1 - 4, Economic Burden criteria	Use IRM referral criteria located in IRM 21.3.5-1, Referral IRM Research List, to refer the taxpayer's issue to the specific employee who previously closed the case. Prepare a Form 4442 following procedures in IRM 21.3.5.4.1, When to Prepare a Referral. Transmit or fax Form 4442 to the specific area based on the <i>AM Case Referral/ Reassignment Listing</i> located on SERP.

Reminder: If there is an issue with when to update a taxpayer's address and what can be updated, refer to IRM 25.23.2.3.7, When to Update the Victim's Address.

- (6) On **open identity theft cases**, do not give out specific account information on the common TIN (when staffing the toll-free lines) unless the caller passes additional/high-risk authentication. For additional information, see IRM 21.1.3.2.4, Additional Taxpayer Authentication. If the caller passes the additional taxpayer authentication, you can provide general information on status updates and information from CII case notes entered on "AMS". Provide a reasonable time frame necessary to complete the processing of the case, general information from the case may be necessary. Fraudulent information may be combined with the TIN owner's information, such as IRP data, account transcripts, etc. Do not provide information during the call from the fraudulent return when there is an open identity theft case. You must document AMS with any information provided to the taxpayer during the call.

Caution: Do not assume that the caller is the true owner of the TIN. If, while completing authentication and/or additional authentication, you are unable to determine that you are speaking with the true owner of the TIN, advise the caller to check their records, terminate the call and use AMS issue/narrative to leave a brief note recording the failed disclosure.

- (7) For calls related to a balance due issue on an open IDTVA control, if the taxpayer states they are receiving a balance due notice because their credit elect from the prior year wasn't applied. Input a TC 470 CC 94 via CC REQ 77 on the module with the balance due to prevent notices and the notice progression to collections. For any other balance due issue on an open IDTVA control not in Status 22, input a TC 470 CC 90 on accounts to prevent balance due notices from generating and preventing offsets into the module. For accounts in Status 22, transfer directly to ACS. See IRM 5.19.1.3.2.1.1, ACS Transfer Information.
- (8) If the taxpayer is calling for the status of their transcript request, Form 4506, Request for Copy of Tax Return, or Form 4506-F, Identity Theft Request for Copy of Fraudulent Tax Return, **and** received the **Form 14611**, RAIVS/IVES IPSU, from the RAIVS unit, refer to IRM 25.23.12.4.5, Identity Theft - Transcript Request.
- (9) If the taxpayer is calling only to check on the status of their refund and no additional information is provided, then provide an update on the status of the case including a reminder of the identity theft time frames. In an attempt to minimize frustration a statement like this one could be provided:
"Identity theft is a challenging and ever-changing issue and the IRS is

25.23 Identity Protection and Victim Assistance

committed to working with victims like you to resolve tax-related identity theft cases. The IRS takes identity theft seriously and is committed to resolving identity theft cases as quickly as possible and are taking steps to reduce this timeframe. You will receive notification once your case has been resolved."

- (10) Advise that most cases are resolved in 120 days or less but due to extenuating circumstances caused by the pandemic our identity theft inventories have increased dramatically. On average it is taking us 582 days to resolve identity theft cases. Explain that identity theft cases are worked in the order they are received. If the taxpayer has further questions on the timeframe, advise the taxpayer to visit the IRS.gov web address and type "Processing Status" in the search bar to check the current operational status.

Note: If the time frame above has elapsed, apologize to the taxpayer and explain the processing delays are due to challenges faced over the last couple years. See IRM 25.23.2.2.3, IDT Case Processing Time Frames.

Reminder: If the taxpayer has not yet filed a return and tax-related identity theft is indicated, see IRM 25.23.12.4, Tax-Related Identity Theft.

- (11) If you are unable to assist the taxpayer by responding to their questions and concerns as it relates to the open IDTVA case, use the *IDTVA Employee Lookup* tool to find the controlling IDTVA employee's contact information. Provide the taxpayer with the IDTVA toll-free number (855-343-0057) or IDTVA International telephone number (267-941-1000), IDTVA's employee's name, six-digit extension and Tour of Duty (TOD), and availability based on the taxpayer's time zone.

Advise the taxpayer of the following:

- *"If you receive the employee's voice mail, leave a brief message to identify yourself and provide your telephone number. Your call will be returned within five (5) business-days. The five business-days will begin the day after the message was left".*
- *"If you do not receive a call back within five (5) business-days, call back on the identify theft toll-free number (800-908-4490) and advise the IRS employee answering the call that you had left a message for the assigned employee and have not received a call back within five business-days. That employee will follow-up on the call back request."*

Exception: If the IDTVA controlling employee's extension is not available using the **IDTVA Employee Look-up** tool, refer the taxpayer's inquiry using a secure email to the employee and the employee's manager using a secure email link. Advise the taxpayer a call will be returned within five (5) business-days. If you do not receive a call back within five (5) business-days, call back on the identify theft toll-free number (800-908-4490) and advise the IRS employee their inquiry was referred to the assigned employee and they have not received a call back within five business-days. That employee will follow-up on the call back request. Explain to the taxpayer the IRS is experiencing higher than normal inventory levels since the pandemic occurred. We are committed to working with victims like themselves to resolve our identity theft inventory. Apologize for any inconvenience these delays are causing. Refer to paragraph 8 above for suggested timeframe statement to provide the taxpayer.

Note: If the processing time frame above has elapsed and the Identity Theft claim remains unassigned, **reassign** the case to the IDT holding number “1174078935” and follow procedures in IRM 21.5.1.5.2, Cases Currently Assigned in CII, for reassignment procedures. This will ensure the taxpayer’s claim is properly assigned to an IDTVA employee. Explain the processing timeframe has elapsed, and the case requires assignment to an IDTVA employee. Inform the taxpayer that a referral will be sent to have their case assigned to an employee. If the taxpayer has further questions regarding the timeframe, please refer to paragraph 9 above.

(12) After you have provided the information above to the taxpayer on their open or closed case, including sending a secure email or referral (Form 4442), you must update AMS to document the call and the information the taxpayer provides:

- The letter or notice (example: Letter 4674C/4674SP, Letter 4675C/4675SP, Letter 5064C or CP 01C or CP 01C (SP) etc.) the taxpayer is inquiring about.
- Document the DLN of the return the caller authenticated if the tax year/module in question contains multiple returns.
- A telephone number(s) where the taxpayer can be reached and the best time for the IDTVA employee to contact them.
- The date the caller filed the tax return and the amount of refund expected (when applicable).
- Include other pertinent information filed on the return that will assist the IDTVA employee in resolving the case.

Example: If the TIN was stolen and used on a fraudulent return or the refund amount they received is not what they were expecting.

Note: An AMS narrative must be entered if a secure email is issued:
“Secure email sent.”

(13) If a taxpayer calls and indicates they have not received a call back within five business-days, please see IRM 25.23.12.4.2 Open Identity Theft Victim Assistance (IDTVA) Controls – Call Back not Received by Taxpayer.

25.23.12.4.2
(10-01-2020)
**Open Identity Theft
Victim Assistance
(IDTVA) Controls - Call
Back not Received by
Taxpayer**

(1) If a taxpayer calls and indicates they have not received a call back within five business-days:

- Try to answer the taxpayer’s questions.
- Research and verify through AMS the call and contact information (employee’s name, extension and TOD) was provided to the taxpayer and at least five business-days has passed since the day after the taxpayer left a message requesting a call back.

Example: A taxpayer calls on a Monday and leaves a message on IDTVA employee Mr. Smith’s extension, requesting a call back. The five business-days starts the day after the message is left which is Tuesday. The taxpayer would need to wait until the following Monday before stating they did not receive a call back.

- Search AMS for indications the IDTVA employee attempted to contact the taxpayer. If the employee has attempted contact, advise the

25.23 Identity Protection and Victim Assistance

taxpayer of those attempts and of any action the employee may have taken, such as sending the TP a letter or similar closing actions.

- (2) If you are unable to assist the taxpayer, advise the taxpayer that you will follow-up to have their call returned within two business-days.
- (3) Use the *IDTVA Employee Lookup* tool to find the controlling IDTVA employee's contact information. Issue a secure email to the employee and their manager, with a copy (CC) to the assigned P&A analyst. Advise them the call must be returned no later than the next business-day.

Exception: If the controlling employee's IDRS Number is not available and a secure email was previously issued, provide detailed information related to the history in a follow-up secure email.

Note: When using the IDTVA Employee Look-Up Tool, the employee's, manager's and P&A analyst's names and email addresses are systemically included in the required email.

25.23.12.4.3
(09-04-2018)

Identity Theft - Freeze Codes

- (1) Refer to IRM 21.5.6, Freeze Codes, for guidance specific to freeze codes.

25.23.12.4.4
(10-30-2020)

Identity Theft - Refund Inquiries

- (1) For most calls, refer to the subsections under IRM 21.4, Refund Inquiries. However, if research of the taxpayer's account shows a systemic true duplicate condition along with an indication of an external data breach (TC 976, TC 971 AC 142, TC 971 AC 123 PREPARER CONTACT and/or a TC 971 AC 125), see IRM 25.23.12.4.4.1, Identity Theft Cases from External Data Breaches for guidance on how to complete a Form e-4442.
- (2) If the taxpayer's call is regarding their Economic Impact Payment (EIP), research the account to confirm the issuance of an EIP. See IRM 21.6.3.4.2.13.2, Economic Impact Payments – Refund Inquiries.

25.23.12.4.4.1
(10-01-2025)

Identity Theft Cases from External Data Breaches

- (1) There are some instances where identity theft claims are resolved incorrectly when the taxpayer is a victim of an external data breach.
- (2) Identity theft resulting from external data breaches may be challenging to recognize, but careful and thorough research must be performed to ensure we don't treat those returns as true duplicates or reject valid claims. In the worst-case scenario, a fraudster obtained completed but unfiled tax returns from a tax return preparer's computer system. Because of this, the identity theft returns are the same as the SSN owners' returns except for the direct deposit information; they are identified as systemic true duplicate. See IRM 25.23.1.7, Taxpayers who are Victims of a Data Breach.
- (3) A CSR may receive calls from taxpayers inquiring about their refunds and there may be evidence of a systemic true duplicate filing condition involving an external data breach incident. Characteristics can be identified on the SSN account with the following:

#

#

- (4) If research confirms the taxpayer is a victim of identity theft as a result of an external data breach, and some of the characteristics listed above are present on the taxpayer's account follow procedures in paragraph (5) below.
- (5) Follow the steps below to prepare a referral, e-4442, to IDTVA.

Step	Action
1	Create an e-4442 on AMS using the following information along with other required fields, Referral Type: IRM. From the IRM drop down menu, select " Other-write-in "; enter IRM 25.23.12.4.4.1 Reason field , select Complex Issue/Training Specialization See IRM 21.3.5.4.2.1.1, Preparing an e-4442, for guidance on creating an e-4442.
2	Clearly note a valid/correct address in the appropriate field of the e- 4442 if, after verifying disclosure, the taxpayer has confirmed a different address than what is on Master File (MF).

Step	Action
3	<p>Provide a detailed narrative in the “Taxpayer Inquiry/ Proposed Resolution” field explaining the taxpayer’s situation including the following comments: “TP appears to be a victim of an external data breach”.</p> <p>Include the fax number the referral will be sent to from the “<i>Identity Theft - Accounts Management Case Referral/ Reassignment Listing</i>” under the Who/Where tab on SERP</p> <p>Note: Use the TC 976 DLN when determining where to fax the Form 4442.</p> <p>Exception: If there is already an open IDTVA control, see IRM 25.23.12.4.1, Telephone Inquiries Regarding Identity Theft Victim Assistance (IDTVA) Tax-Related Cases. If a different open control is identified (example: TPRQ, DUPF, XRET, etc.), in the “Proposed Resolution” field, include in your recommendation the case be re-assigned to IDTVA immediately.</p>
4	Send the referral along for the systemic approval path.

- (6) Inform the taxpayer a referral will be issued to an employee who will review and resolve the issue identified. Provide the appropriate time frame and apology per IRM 25.23.2.2.3, IDT Case Processing Time Frames.

25.23.12.4.5
(10-16-2023)

Identity Theft - Transcript Requests

- (1) Refer to IRM 21.2.3.5.8, Transcripts and Identity Theft, for guidance specific to requests involving the taxpayer’s filed return(s) and accounts with identity theft. Refer to IRM 25.23.12.5, Responses to Requests for copies of Fraudulent Return(s) for Identity Theft Victims, when the taxpayer requests a copy of the fraudulent tax return. Refer to the table below when the taxpayer is calling for the status of their request for a copy of a tax return.

If	And	Then
<p>Taxpayer is calling for the status of their request for a copy of a tax return filed on</p> <ul style="list-style-type: none"> Form 4506, Request for Copy of Tax Return or Form 4506-F, Identity Theft Victims Request for Copy of Fraudulent Tax Return 	<p>They did receive the Form 14611, RAIVS/ IVES Additional Actions Needed.</p>	<p>Refer to IRM 21.3.6.4.3.2, Return Copy Procedures and Identity Theft for additional guidance.</p>

If	And	Then
Taxpayer is calling for the status of their request for a copy of the fraudulent return filed on Form 4506-F,	They did not receive the Form 14611 from RAIVS/IVES.	Refer to IRM 25.23.12.5, Responses to Requests for copies of Fraudulent Return(s) for Identity Theft Victims.

25.23.12.4.5.1
(11-05-2024)

**Transcript NOT
Requested - Taxpayer
Claims Identity Theft**

- (1) If the taxpayer indicates receipt of a transcript they did not request, probe to determine if their spouse or someone who is authorized (such as a tax professional, power of attorney, or financial institution, etc.) could have requested the transcript.

Note: If the taxpayer is calling about a Form 14611 they received, see IRM 21.2.3.5.8, Transcripts and Identity Theft.

Reminder: Using EUP/TDS, “View Transaction History” displays the date and entity information for when the transcript is requested. Compare this with the information provided by the taxpayer for assistance in probing and re-searching.

- (2) Once it is confirmed neither the taxpayer, nor the taxpayer’s spouse, or any other authorized representative requested the transcript in the mail, apologize and explain that someone had enough information to request the transcript through our system, but did not receive the transcript. Thoroughly research the SSN(s) on the transcript in question to ensure there is no open or unresolved tax-related identity theft issue.
- (3) If an open identity theft control is identified, see IRM 25.23.12.4.1, Telephone Inquiries Regarding Identity Theft Victim Assistance (IDTVA) Tax-Related Cases, for additional actions and guidance.

Note: See Exhibit 25.23.2-15, IDTVA IDRS Category Controls by Function, for a list of identity theft category control codes.

Reminder: See IRM 25.23.2.4.4.1, IMF Identity Theft - Taxpayer Initiated Allegations of Identity Theft - TC 971 AC 522, and input when appropriate.

- (4) If an unresolved tax related identity theft issue is identified without an open control, see IRM 25.23.12.4.1, Telephone Inquiries Regarding Identity Theft Victim Assistance (IDTVA) Tax-Related Cases, and complete a e-4442 and transmit or fax to the specific area based on the *AM Case Referral/ Reassignment Listing* located on SERP under the Who/Where tab. Provide the taxpayer with a 30 day time frame for contact or resolution. See IRM 21.3.5.4.1, When to Prepare a Referral.

Reminder: See IRM 25.23.2.4.4.1, IMF Identity Theft - Taxpayer Initiated Allegations of Identity Theft - TC 971 AC 522, and input when appropriate.

- (5) If there is no tax-related identity theft on the SSN(s), tell the taxpayer there are currently no identity theft indicators on their tax account. Provide guidance and resource information for identity theft per IRM 25.23.12.2, Identity Theft

Telephone General Guidance. Then refer to IRM 25.23.12.3, Non-Tax Related Identity Theft - Self Identified and provide the taxpayer with information on opting-in or applying to participate in the IP PIN Program to protect their tax account.

- (6) Update AMS history to specify the reason the taxpayer called (example: received transcripts that were not requested).

25.23.12.4.6
(09-04-2018)
**Identity Theft -
Unpostables**

- (1) Refer to IRM 21.5.5, Unpostables, for guidance specific to unpostable transactions.

25.23.12.4.7
(06-10-2024)
**Identity Theft - Balance
Due Issues**

- (1) For calls related to a balance due issue on a closed identity theft issue see IRM 5.19.21.2.1, Identity Theft Claim.
- (2) For calls related to a balance due issue on an open IDTVA control, see IRM 25.23.12.4.1, Telephone Inquiries Regarding Identity Theft Victim Assistance (IDTVA) Tax-Related Cases, paragraphs (5), (6), (7), (8), (9), (10), and (11).

25.23.12.4.8
(10-01-2023)
**Responses to IM Breach
Notification Letter 4281C**

- (1) Refer to IRM 10.5.4.4.7.1, Handling Inquiries About IM Data Breach Notification Letters, for guidance specific to request involving Letter 4281C. Questions regarding the content of IRM 10.5.4, Incident Management Program, should be directed to that IRM owner.

25.23.12.4.9
(10-01-2025)
**Identity Theft -
Economic Impact
Payments (EIP)**

- (1) The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) was signed into law on March 27, 2020. IRC 6428 provides eligible individuals with a recovery rebate credit (RRC) for tax year 2020 that taxpayers may receive as an advance payment. Advance payments of the RRC are referred to as an Economic Impact Payments (EIPs). EIP 1 was required to be paid on or before December 31, 2020. An eligible individual who did not receive EIP 1 before that date would need to claim the amount to which they are entitled as an RRC on their tax year 2020 return.
- (2) A second Economic Impact Payment was included in the Consolidated Appropriations Act, 2021 that was signed into law on December 27, 2020. This increased the Recovery Rebate Credit for the tax year 2020 that taxpayers may receive also as an advance payment. EIP 2 was required to be paid on or before January 15, 2021. An eligible individual who did not receive EIP 2 before that date would need to claim the amount to which they are entitled as an RRC on their tax year 2020 return.
- (3) The American Rescue Plan Act of 2021 was signed into law on March 11, 2021. It provides eligible individuals with a recovery rebate credit for tax year 2021 that taxpayers may receive as an advance payment Economic Impact Payment. EIP 3 was required to be paid on or before December 31, 2021. An eligible individual who did not receive EIP 3 before that date would need to claim the amount to which they are entitled as an RRC on their tax year 2021 return.
- (4) Individuals may call the IRS to report their TIN has been misused to obtain the Economic Impact Payments. All toll-free employees receiving calls should continue to follow basic required authentication procedures using the IAT Disclosure tool to assist callers and prevent unauthorized disclosure of taxpayer

information whenever it is necessary to access a taxpayer's account. When the IAT Disclosure tool alerts the users to account conditions where identity theft is a factor/suspected, documented, or the account involves multiple entities, mixed periods, cases involving open IDT related transactions, MFT 32 accounts, open identity theft controls, etc., additional authentication must be completed before disclosing information. See IRM 21.1.3.2.4, Additional Taxpayer Authentication, for high-risk authentication procedures.

- (5) Guidance should be provided to these individuals identifying themselves or their dependent as a potential victim of tax-related identity theft. This guidance will assist the taxpayer in protecting their identity. Refer to IRM 25.23.12.2(5), Identity Theft Telephone General Guidance.
- (6) Research to determine if a return is on file and the EIPs were issued. If your research determines EIPs were issued and the taxpayer is claiming the return on file was a fraudulent return and they did not receive their EIPs, advise the taxpayer they should submit a claim using Form 14039, Identity Theft Affidavit, when they allege they are victims of tax-related identity theft. See IRM 25.23.2.3, Identity Theft Claims - General Guidelines. If the taxpayer's call is regarding any or all of their Economic Impact Payments (EIP) and they are claiming to be a victim of identity theft, then refer to IRM 21.6.3.4.2.13.2 , Economic Impact Payments – Refund Inquiries and follow any procedures that may apply.

25.23.12.5
(10-01-2025)
**Responses to Requests
for copies of Fraudulent
Return(s) for Identity
Theft Victims**

- (1) The IRS accepts requests for and provides masked copies of fraudulent returns to victims of identity theft or persons authorized to obtain the identity theft information. Requests are accepted and processed for instances where the fraudulent return is filed and accepted for processing using the identity theft victim's name and social security number as a primary or secondary taxpayer.
- (2) When an identity theft victim requests a copy of a fraudulent return filed under their SSN via toll-free call, employees will:
 - Advise the requestor a Form 4506-F, Identity Theft Victims Request for Copy of Fraudulent Tax Return, is required. The form is available to complete and submit online through their Individual Online Account at IRS.gov/account under the Forms page. If the taxpayer doesn't have an online account, ask if they would prefer to receive the information via the internet or over the phone.
 - If the requestor prefers to access the information via internet, then advise that Form 4506-F (with instructions on the back) is available on the IRS website, www.irs.gov, by searching using the form number. Advise the requestor of the FAQs available on www.irs.gov using key words, "identity theft" to search for answers to Frequently Asked Questions regarding identity theft.
 - Provide verbally to the requestor who prefers to obtain the information over the phone the information from the IRS website: *Instructions for Requesting Copy of Fraudulent Returns*.
 - Answer any Non-Tax Law question the caller may have about the form and/or instructions.
 - Explain the form can be mailed or faxed (not both) and then provide the centralized address and fax number:
Internal Revenue Service
Fresno, CA 93888-0025

25.23 Identity Protection and Victim Assistance

or

Include a fax cover sheet marked "Confidential"

Fax this form toll-free to 855-807-5720

Note: If the taxpayer is using a private delivery service (examples: FedEx or UPS etc.) a street address must be provided;
3211 S Northpointe Dr.
Fresno, CA 93725
"Identity Theft - Request for Fraudulent Return"

- Inform the requestor some information on the fraudulent return is redacted or blacked out, but there is enough information to determine how the taxpayer's personal information is used.
 - Explain the IRS cannot provide a copy of the fraudulent return to any person only listed as a dependent, nor can it be provided to that person's/dependent's parent, legal guardian, or authorized representative.
 - Advise the taxpayer most cases are resolved in 120 days or less, but due to extenuating circumstances caused by the pandemic our identity theft inventories have increased dramatically and on average it is taking us 582 days to process these requests. The IRS takes identity theft seriously and is committed to resolving their request as quickly as possible and are taking steps to reduce this timeframe.
 - Answer any additional questions raised by the requestor; do not refer the taxpayer to another phone number.
- (3) When the taxpayer is calling for the status of their Form 4506-F, Request for Copy of Fraudulent Tax Return, and they **did not** receive a Form 14611, RAIVS/IVES IPSU, follow the guidance in the chart below.

If	And	Then
There is an open IDT7 on the taxpayer's account.	There is an open tax-related identity theft as indicated by <ul style="list-style-type: none"> • open IDT(x), IDS(x) (the "x" represents an IDT/S 1, 3, 6, or 8) Or • open IDI(x) (the "x" represents an IDI 1, 3, 4, 5, 6, 8 or 9). Or • an unreversed TC 971 AC 522 with the MISC field code containing UNWORK 	Refer to IRM 25.23.12.4.1, Telephone Inquiries Regarding Identity Theft Victim Assistance (IDTVA) Tax-Related Cases.

If	And	Then
There is an open IDT7 on the taxpayer's account	<p>There is no open tax-related identity theft case and there is resolved IDT as indicated by</p> <ul style="list-style-type: none"> • A posted TC 971 AC 501 or • A posted TC 971 AC 506 or <p>There is no indications of tax-related IDT on the account</p>	<p>Advise the taxpayer most cases are resolved in 120 days or less, but due to extenuating circumstances caused by the pandemic our identity theft inventories have increased dramatically and on average it is taking us 582 days to process these requests.</p> <p>Note: If the time frame above has elapsed and a 5835C Letter has not been sent, apologize to the taxpayer and explain the processing delays due to challenges faced over the last couple years. See IRM 25.23.2.2.3, IDT Case Processing Time Frames.</p> <p>Note: If a 5835C Letter has been sent, regardless of timeframe, see paragraph 8 of IRM 25.23.12.4.1, Telephone Inquiries Regarding Identity Theft Victim Assistance (IDTVA) Tax-Related Cases, to provide IDTVA employee contact information.</p>

- (4) If the taxpayer is calling for the status of their transcript request, Form 4506-F, Identity Theft Victims Request for Copy of Fraudulent Tax Return, and received Form 14611, RAIVS/IVES IPSU, in the mail from the RAVIS unit, refer to IRM 21.2.3.5.8, Transcripts and Identity Theft, and IRM 21.3.6.4.3.2, Return Copy Procedures and Identity Theft for additional guidance.

25.23.12.6
(10-01-2025)
IP PIN Program
Telephone Inquiries

- (1) Participating in the IP PIN Program is voluntary for taxpayers who are not victims of tax-related identity theft. To find out if a taxpayer is eligible to opt-out, they would need to log into their Individual Online Account. IRS employees can assist taxpayers on how to access the Individual Online Account web page to enroll or view their online account located at <https://www.irs.gov/your-account>. Taxpayers can see the Online Account for Individuals – Frequently asked questions for more information regarding features of the Individual Online Account. Taxpayers having trouble accessing or creating an account for an IRS online service can visit *How to Register for Certain Online Self-Help Tools* or should be directed to the *IRS ID.me Help Center*. Taxpayers having trouble accessing or creating an account for an IRS online service can visit or should be directed to the website by visiting <https://help.id.me>.

#

Note: If necessary, advise taxpayers that once an opt-out selection is made, taxpayers will need to allow up to 72 hours before they can electronically file without an IP PIN. The same timeframe applies if the taxpayer wants to opt back into the IP PIN program.

Ways to Enroll	Description
1. Automatic Enrollment	Taxpayers who have been confirmed victims of tax-related identity theft will have an indicator placed on their account which places them into the IP PIN Program automatically. See IRM 25.23.2.9.1.1, Automatic Enrollment in the IP PIN Program, for more information.

#

Ways to Enroll	Description
3. Electronically, Mailing or Faxing Form 15227, Application for an IP PIN	Taxpayers can apply for an IP PIN by submitting Form 15227, Application for an Identity Protection Personal Identification Number (IP PIN), electronically, by mail or fax. See IRM 25.23.3.2.7, Application for an Identity Protection Personal Identification Number (IP PIN) Overview - Form 15227, for eligibility.
4. Visiting a Taxpayer Assistance Center (TAC) for an IP PIN Appointment	Individuals may call the IRS TAC toll-free appointment line (844-545-5640) to request a TAC appointment in an effort to obtain an IP PIN. After taxpayers verify their identity at their local TAC, they are enrolled into the IP PIN Program. See IRM 25.23.2.9.1.3, IP PIN TAC Appointment Procedures for when to make an appointment for the TP. Note: Visiting a TAC for an IP PIN Appointment is only available for applicants who reside in the US.

Reminder: Do not suggest filing a Form 15227 or schedule TAC appointments for taxpayers who are requesting a re-issuance of their IP PIN due to lost, misplaced, or non-receipt. See IRM 25.23.2.9.4.1, Lost, Misplaced or Non-Receipt of IP PIN.

- (2) If the taxpayer is calling regarding lost, misplaced or non-receipt of their or their dependent's annual IP PIN Notice CP 01A, you **must** attempt to access and research the taxpayer's account.
- Perform authentication including additional authentication of the caller if it is required while using the IAT Disclosure Tool, see IRM 25.23.12.2, Identity Theft Telephone General Guidance, for additional disclosure guidance for dependent related IP PIN inquiries.
- Note:** If a call is received from third party who indicates they have a third party authorization on file or is submitting a new or original authorization, follow procedures in IRM 21.1.3.3, Third Party (POA/TIA/F706) Authentication.

Caution: IP PINs are assigned to an individual's TIN. IP PIN indicators are considered personal account information and are specific to the individual taxpayer on joint tax accounts. If a taxpayer calls to confirm their spouse's account status of an IP PIN or

to obtain their spouse's IP PIN, the procedures in IRM 21.1.3.3, Third Party (POA/TIA/F706) Authentication, must be followed.

- Confirm the taxpayer's account reflects an IP PIN indicator was generated (IP PIN:1 on CC IMFOLE), see IRM 25.23.2.9.2, Identifying If a Taxpayer has an IP PIN Requirement.
- Determine if any account conditions prevented the issuance of the notice, see IRM 25.23.2.9.3, Receiving and/or Retrieving your Annual IP PIN.
- Research to determine that **ALL** the statements in IRM 25.23.2.9.4.1, Lost, Misplaced or Non-Receipt of IP PIN, (4) are true and the taxpayer is eligible for re-issuance of their IP PIN.
- If all statements are true, inform the taxpayer we can re-issue their IP PIN via a Letter 4869C within 21 calendar days and re-issue the IP PIN using the IP PIN Entry Tool. Inform the taxpayer that they may obtain/view their IP PIN faster by accessing their Individual Online Account located online at www.irs.gov/your-account. See IRM 21.2.1.62(4), Individual Online Account. The IP PIN will be viewable on the Profile page of their account. Also, a digital copy of the CP 01A containing their IP PIN may be available in the Notices section of their account. Please see IRM 25.23.2.9.4, Lost, Misplaced or Non-Receipt of IP PIN Overview for the IP PIN Entry Tool.

#

Reminder: During the call, inform the taxpayer that if they do not receive their re-issued IP PIN letter within 21 calendar days filing by paper would be their only option. Advise the taxpayer a paper return with a missing or incorrect IP PIN is subjected to additional review for identity verification, which will delay return processing and issuance of any refund that may be due.

- If all statements are not true, advise the taxpayer their only option is to file a paper return and apologize for the inconvenience. Advise the taxpayer a paper return with a missing or incorrect IP PIN is subjected to additional review for identity verification, which will delay processing their return and issuance of any refund that may be due.

#

- Advise the taxpayer if they change their address prior to the next filing season, they must complete Form 8822, Change of Address (prior to the start of the next tax season). The form is available by visiting www.irs.gov/f8822. If a parent or legal guardian of a minor dependent calls requesting dependents IP PIN be re-issued remind the parent/guardian that in the future, any change of address impacting the dependent re-

25.23 Identity Protection and Victim Assistance

quires the submission of a Form 8822, Change of Address. This should be completed using the dependent's TIN and name.

- (3) Answer any general questions the caller may have related to the IP PIN program before accessing a taxpayer's account. There may be times you may not need to access the caller's account to respond to general questions. General questions may include: (this list is not all inclusive)

- What is an IP PIN/IP PIN Program?
- How does the IP PIN Program protect me?
- If I enroll, can I opt-out of the IP PIN Program at any time?
- Who's eligible for an IRS IP PIN?
- Can I use my current IP PIN on a prior year tax return?

25.23.12.6.1

(10-01-2025)

Responding to Telephone Inquiries Regarding Form 15227 for Obtaining an IP PIN

- (1) The IRS offers a few options for taxpayers or authorized person to apply and obtain an IP PIN. Participating in the IP PIN Program is voluntary for individuals who are not victims of tax-related identity theft. All individuals with an SSN or an ITIN are eligible to opt into the IP PIN program. The fastest way for an individual to enroll in the IP PIN Program is by opting in using the Individual Online Account at www.irs.gov/your-account. Individuals who do not already have an account must register by verifying their identity. Once enrolled, they can immediately view their IP PIN on the Profile page of their account. See IRM 25.23.2.9.1, Participating in the IP PIN Program.
- (2) When a taxpayer calls to inquire about the IP PIN paper application process, employees will:
- Advise the taxpayer a Form 15227, Application for an Identity Protection Personal Identification Number (IP PIN), is required. Form 15227 is available online for download or can be electronically submitted through <https://www.irs.gov/dmaf/form/f15227>.
 - If the taxpayer prefers to view the information online for how the IP PIN paper process works, advise the taxpayer the information can be found on the IRS website at www.irs.gov/ippin. Advise the taxpayer to visit <https://www.irs.gov/dmaf/form/f15227> for instructions and electronic completion of the IP PIN application. After filling in the form, they will have the option to submit it online or download a copy for mailing.
 - If the taxpayer does not have access to the internet or prefers to obtain the information over the phone, verbally provide the taxpayer with the filing requirements for submitting Form 15227. Provide the toll-free number they can call and order the form; 800-829-3676.

#

- Explain if not submitting the Form 15227 online through <https://www.irs.gov/dmaf/form/f15227>, the form can be mailed or faxed (not both). Provide the centralized address or fax number listed under the Instruction section of Form 15227.

Note:

Where to mail Form 15227	Where to fax Form 15227
<p>If submitting Form 15227 by mail: Department of the Treasury, IRS Fresno, CA 93888-0025</p> <p>If using a private delivery service (Fed Ex or UPS), provide the following street address: Department of the Treasury, IRS 3211 S Northpointe Dr. Fresno, CA 93725</p>	<p>If submitting Form 15227 by fax: Include a cover sheet marked 'Confidential' Fax to the toll-free number 855-807-5720</p>

- Advise the taxpayer our online services Do Not provide information on the status of their Form 15227 application. Provide taxpayers with a realistic expectation of the time frame for resolution of their application. Apologize to the taxpayer for the length of time required to process their request. Suggested language is: Most cases are resolved in 120 days or less but due to extenuating circumstances caused by the pandemic our inventories have increased dramatically. On average it is taking us 582 days to process some applications. We are committed to processing your application as quickly as possible and are taking steps to reduce this timeframe.
 - Explain to the taxpayer once they have been approved to receive an IP PIN using the Form 15227 process they will receive two notices, a 4403C Letter confirming approval of their application and a Notice CP01A containing their IP PIN, in the next 4 to 6 weeks.
 - Answer any additional questions raised by the taxpayer; do not refer the taxpayer to a different toll-free number.
- (3) When an individual calls and indicates they have applied for an IP PIN using Form 15227 and they are requesting a status update, employees will:
- Perform authentication including additional authentication of the caller as required using the IAT Disclosure Tool, see IRM 25.23.12.2, Identity Theft Telephone General Guidance, for additional disclosure guidance for dependent related IP PIN inquiries.
 - Research and verify through AMS that the application was received and if any additional information was requested from the requestor. If no information is available, then advise the taxpayer to allow at least 120 days from the date they submitted online, mailed, or faxed their Form 15227. Apologize to the requestor and provide with a realistic expectation of the time frame for resolution of their application. Suggested language is: Most cases are resolved in 120 days or less but due to extenuating circumstances caused by the pandemic our inventories have increased dramatically. On average it is taking us 582 days to process some applications. We take identity theft seriously and are committed to processing your application as quickly as possible and are taking steps to reduce this timeframe.

25.23 Identity Protection and Victim Assistance

- Research AMS for indications the IDTVA employee attempted to contact the taxpayer. If the employee has attempted contact, advise the taxpayer of the attempts. Using the *IDTVA Employee Lookup* tool to provide IDTVA employee's contact information, advise the taxpayer they will be receiving an acknowledgement letter via mail, and request the best time for a call back. Enter the information obtained on AMS.
 - Attempt to answer the taxpayer's questions.
- (4) If you are unable to assist the taxpayer, use the *IDTVA Employee Lookup* tool to find the controlling IDTVA employee's contact information. Verify with the taxpayer they have the correct name and extension for the controlling IDTVA employee. Recommend they try calling the number again. Issue a secure email to the employee and their manager including a copy (cc) to the assigned P&A Analyst. In the email, advise the employee that a return call to the requestor (applicant) must be returned no later than the next business day.

Note: When using the IDTVA Employee Look-up Tool, the employee's, manager's and P&A analyst's names and email addresses are systemically included in the required email.

- (5) Advise the requestor you have sent a follow-up email to the assigned employee to have their call returned within two (2) business days.
- (6) If the identity theft case is closed, you may provide updated information related to their application for an IP PIN to the TIN owner or authorized representative (e.g., Form 8821 Tax Information Authorization or Form 2848 Power of Attorney and Declaration of Representative) utilizing normal procedures.
- If an IP PIN was provided to the TIN owner as requested, it can usually be identified by the following transaction(s) on IDRS via CC ENMOD and/or CC IMFOLE:
A posted TC 971 AC 528 with the MISC field code TS IPSU TPRQ and, A Letter 4403C was issued to the taxpayer using Required Letter Scenarios 15 in IRM Exhibit 25.23.3-2, Identity Protection Personal Identification Number Paper Application Scenarios for the 4403C and 4403SP Letter.
 - If an IP PIN was denied, it can be identified by the following:
A Letter 4403C was issued to the taxpayer using any of the following Required Letter Scenarios 2, 3, 4, 5, 6, 8, 12, or 13 in IRM Exhibit 25.23.3-2, Identity Protection Personal Identification Number Paper Application Scenarios for the 4403C and 4403SP Letter.
 - If the taxpayer filed a Form 15227 as the parent or legal guardian and it was rejected due to failing authentication, IDTVA employees may request additional documentation. Refer to the table in IRM 25.23.4.8.4.1(3), Dependent Related Identity Theft (IDT) – Determinations, for a list of acceptable and unacceptable documentation

Note: Case Notes on CII should be viewable on AMS. You can research the Case Notes on AMS for the IDTVA employee's final determination.

- (7) Document the call and all actions taken on individuals account on AMS or CII case notes. Case actions on CII systemically post a note to AMS. See IRM 25.23.2.3.4, Required Case and History Notes.

25.23.12.6.2

(10-01-2025)

**Identity Protection
Personal Identification
Number (IP PIN) TAC
Appointment Request
Received on Toll-Free
Account Lines (App
20/21, 161/162)**

- (1) Individuals may call the IRS to request an appointment in an effort to obtain an IP PIN. Complete research must be completed on the TIN provided to determine if the taxpayer is already enrolled in the IP PIN program, if there is an open IDT control or other issues that prevents the individual from receiving one. If there is an open control advise the individual, they must wait until the IDT case is resolved as an IP PIN may be assigned.

If there is an Open	Then
IDT control (ex: IDT1/3/4 etc. or IDI1/2/3 etc.)	<ul style="list-style-type: none"> On open identity theft cases, do not give out specific account information on the common TIN unless the caller passes additional/high-risk authentication. Telephone CSRs must not adjust or take any account actions on open identity theft accounts. See IRM 25.23.12.4.1, Telephone Inquiries Regarding Identity Theft Victim Assistance (IDTVA) Tax-Related Cases, for additional guidance if you are unable to assist the taxpayer in responding to their questions or concerns as it relates to the open IDTVA case.
IDTX control	<ul style="list-style-type: none"> On open IDTX cases, do not give out specific account information on the common TIN unless the caller passes additional/high-risk authentication. Review IDRS to see if the IDTX case has been assigned to an IDTVA employee and if any actions have been taken on the account. If the caller passes the additional taxpayer authentication, you can provide general information and status updates from the CII case notes entered on "AMS". If they are calling to provide additional information to assist in resolving their application on Form 15227, Application for an Identity Protection Personal Identification Number (IP PIN), or to confirm IRS employee tried to contact them, utilize the IDTVA Employee Lookup Tool, provide the contact information for the employee assigned to their IDTX case and confirm the individual is an IRS employee. See IRM 25.23.12.4.1, Telephone Inquiries Regarding Identity Theft Victim Assistance (IDTVA) Tax-Related Cases.

If there is an Open	Then
IDTX control on a minor dependent's TIN	<ul style="list-style-type: none"> On an open IDTX cases control under a minor's TIN, do not give out specific account information on the TIN until you have determined the caller is eligible to receive the information. Conduct complete research to determine the relationship of the caller/requestor, (parent or legal guardian of the minor dependent), to the applicant listed on Form 15227 using CC DDBKD. If you can confirm through your research that the caller/requester is the parent/legal guardian of the applicant and acting on behalf of the minor dependent, use the TIN of that individual (parent/legal guardian) for required authentication and additional taxpayer authentication. Then have the parent/legal guardian confirm the TIN, Name, Address, and Date of Birth for the applicant for whom the form was filed. Update CII case notes accordingly. Note: Refer to Pub 17, Your Federal Income Tax (For Individuals), Part One, Chapter Three, Dependents, for a situation where a taxpayer may be eligible to authenticate on behalf of their dependent qualifying child or relative regardless of age. Only after you have confirmed the caller identity and they pass the additional taxpayer authentication can you provide general information and status updates from the CII case notes entered on "AMS". Review IDRS to see if the IDTX case has been assigned to an IDTVA employee and if any actions have been taken on the account. If the caller is providing additional information to assist in resolving a Form 15227 application received for their minor dependent, utilize the IDTVA Employee Lookup Tool, then provide the contact information for the employee. See IRM 25.23.12.4.1, Telephone Inquiries Regarding Identity Theft Victim Assistance (IDTVA) Tax-Related Cases.
Any control other than IDT	<ul style="list-style-type: none"> See IRM 21.3.5.4.1, When to Prepare a Referral, to determine if the subject specific IRM sections directs you to prepare a Form 4442/e-4442, Inquiry Referral.

- (2) For individuals requesting an IP PIN, ask if they attempted to use any of the alternative options available to obtain an IP PIN.

#

If your research determines the taxpayer is already enrolled in the IP PIN program, refer to IRM 25.23.2.9.4.1, Lost, Misplaced, or Non-Receipt of IP PIN.

If they respond	Then
1. No	<ul style="list-style-type: none">• Advise them enrolling using “Individual Online Account” tool on irs.gov is the fastest way to receive an IP PIN and provide the website.• If the individual is unable to access the online tool and meets the adjusted gross income criteria for filing the Form 15227, Application for an Identity Protection Personal Identification Number (IP PIN), recommend filing the form.• If the individual’s adjusted gross income on their federal tax return is above \$ 84,000 (any filing status other than married filing joint) or \$ 168,000 (filing status of married filing joint), or they insist on scheduling an appointment, then advise the individual you must provide them the TAC toll-free appointment line number (844-545-5640) to request an appointment for an IP PIN. Note: Visiting a TAC for an IP PIN Appointment is only available for applicants who reside in the US.

#####

If they respond	Then
<p>3. Yes, they filed a Form 15227 and received a Letter 4403C advising them we were unable to process their IP PIN request</p>	<ul style="list-style-type: none">• Research the individual's TIN to determine if there is an open IDTX case or an IDTX case closed on record within the last 12 months (a 4403C closing letter was issued) due to failed attempts to reach the taxpayer, utilize the IDTVA Employee Lookup Tool and provide them with the contact information for the employee. See IRM 25.23.12.4.1, Telephone Inquiries Regarding Tax-Related IDTVA Cases.• If your research identifies a closed IDTX case and the Letter 4403C advises the individual to schedule an appointment at a TAC to authenticate their identity, provide the individual with the TAC toll-free appointment line number (844-545-5640) to request an appointment for an IP PIN and advise the individual of the forms of identification/documentation they are required to bring to a TAC appointment for an IP PIN in paragraph (3) below. <p>Note: Visiting a TAC for an IP PIN Appointment is only available for applicants who reside in the US.</p>

- (3) Advise the individual what forms of identification and/or documentation are required when applying for an IP PIN in person at the TAC:

Who must present forms of Identification/Documentation	Identification/Documentation Required for IP PIN Application TAC Appointment
1. An Individual applying for an IP PIN must present a valid, current U.S. federal or state, government issued form of a picture identification such as:	<ul style="list-style-type: none"> • A driver's license • State identification card • Passport <p>Reminder: Any current US federal or state government issued identification presented MUST be signed by the issuing agency and/or the individual where appropriate.</p>
2. They must provide at least one additional form of identification such as:	<ul style="list-style-type: none"> • A driver's license • State identification card • Passport • Social Security Card • Car Title • Voter Registration Card • Mortgage Statement • Lease agreement for rental domicile • Utility Bill matching address of ID • Birth Certificate (Requires Name at Birth, Date of Birth, and City of Birth) • School Records <p>Note: IRS no longer accepts Puerto Rican birth certificates issued before July 2010, due to new laws by the Government of Puerto Rico. Individuals with birth certificates issued before this date must get new documentation from the Puerto Rico Vital Statistics Record Office.</p>

Who must present forms of Identification/Documentation	Identification/Documentation Required for IP PIN Application TAC Appointment
<p>3. If the appointment is for a dependent IP PIN, the requestor must show proof of their identity from the list above and must provide at least two forms of identification for the applicant if The individual is a minor dependent (under the age of 18) Or The individual advises the employee they do not have a photo identification and they explain this is due to their religious beliefs, members of certain religious sects (Amish, Mennonite, and others)</p>	<ul style="list-style-type: none"> • Birth Certificate (Requires Name at Birth, Date of Birth, and City of Birth) • Bank Statements • Social Security card • Student Records (grade/ high school/college) <p>Note: Accept school records from the last year completed plus one other item from the list.</p> <ul style="list-style-type: none"> • Approved copy of Form 4029, Application for Exemption from Social Security and Medicare Taxes and Waiver of Benefits • Document (on Letterhead) from Health Care Provider (Doctor, Nurse, or clinic) and must have the following information verifying identity of individual: <ul style="list-style-type: none"> • Full Name of Taxpayer (including Parent or Guardian if minor/student) • Address, city, state, zip • Date of Birth • Date and Signature of Health Care Provider (doctor, nurse, or clinic)

Reminder: Visiting a TAC for an IP PIN Appointment is only available for applicants who reside in the US.

Note: If the caller states they only have a picture identification issued by a foreign country, follow IRM 3.21.263.6.3.4.2, Reviewing Supporting Identification Documents, and IRM 3.21.263.6.3.4.2.1, Supporting Identification Document Certification Requirements.

- (4) Document call and all actions taken on individuals account on AMS or CII case notes. Case actions on CII systemically post a note to AMS. See IRM 25.23.2.3.4, Required Case and History Notes. Once all documentation and actions are complete, offer to transfer the caller to App 55 / 56 to schedule an appointment.

25.23.12.6.3

(04-23-2025)

**Responding to
Telephone Inquiries
Regarding ID.me**

- (1) The Internal Revenue Service (IRS) works with ID.me, a credential service provider, to provide authentication and identity verification for taxpayers and tax professionals accessing IRS applications including Individual Online Account, Online Payment Agreement, Tax Pro Account, e-Services, Submit Forms 2848 and 8821 Online, and Get an Identity Protection PIN (IP PIN). Users prove their identity by uploading government documents, taking a video selfie, and filling out personal information. These identity verification services are crucial for the IRS to ensure millions of taxpayers and tax professionals can securely access IRS online services.
- (2) IRS employees cannot assist taxpayers in creating an ID.me account. Do not refer taxpayers to the Electronic Products & Services Support (EPSS) help desk for assistance with creating an ID.me account.
- (3) Taxpayers having trouble accessing or creating an account for an IRS online service can visit *How to Register for Certain Online Self-Help Tools* or should be directed to the *IRS ID.me Help Center* website by visiting <https://help.id.me>

Note: Taxpayers verifying through video chat must return to IRS.gov to access the online service upon successfully completing the process.

- (4) Follow the chart below when a taxpayer reports an ID.me account was created fraudulently, or their account was compromised.

If	And	Then
1. Taxpayer is reporting an ID.me account was created fraudulently or their account was compromised	They did receive a CP 303 notice from the IRS.	<ul style="list-style-type: none"> • Advise the taxpayer to immediately call the number provided on their CP 303 notice. • Advise them once their identity has been verified their online account will be disabled.

If	And	Then
2. Taxpayer is reporting an ID.me account was created fraudulently or their account was compromised	They did not receive a CP 303 notice from the IRS	Advise the taxpayer to immediately report it to ID.me. Refer them to the <i>Privacy & Fraud</i> section of the <i>ID.me Help Center</i> . Taxpayers can use key words “reporting identity fraud” in the search section for steps to report the suspected fraud.

- (5) Refer to *ID.me Help pages* for a visual tutorial on creating a new ID.me account. If the link does not work, you may access the tutorial in SERP Job Aids under Direct File.

25.23.12.7
(10-01-2025)
**Rescind – Form 14039
Identity Theft Affidavit**

- (1) If the taxpayer states their Form 14039, Identity Theft Affidavit was filed in error, or the taxpayer wants to rescind their claim, perform authentication including additional authentication of the caller as required using the IAT Disclosure Tool, see IRM 25.23.12.2, Identity Theft Telephone General Guidance, for additional disclosure guidance for dependent related IP PIN inquiries.

Note: If call is received from third party who indicates they have a third party authorization on file or is submitting a new or original authorization, follow procedures in IRM 21.1.3.3, Third Party (POA/TIA/F706) Authentication

- (2) Confirm the taxpayer’s account to determine if it contains a TC 971 AC 522 UNWORK or PNDCLM. Research the account for any unresolved TPP issues, MFT 32, multiple entities, mixed periods, cases involving IDT related transactions, and open identity theft controls for the tax period(s) the claim was filed for.
- (3) Review the account to determine if there’s an identity theft issue open in another function. If there is an open identity theft case, refer the case to that function using your normal referral procedures. Do not take actions on identity theft cases being worked by another function. If there is no open issues, the taxpayer is eligible to rescind their identity theft claim.
- (4) Ask probing questions to determine why the taxpayer is requesting to rescind their identity theft claim and document AMS, or the case history if you do not have access to AMS, with the taxpayer’s response. For example, “Can you provide the reason why you would like to rescind your identity theft claim?” Explain to the taxpayer by allowing the identity theft claim to process, if determined to be a victim of identity theft, it will:
1. Help prevent future identity theft incidents.
 2. Ensure any returns filed are reviewed for identity theft indications.
- (5) Inform the taxpayer that they can protect their account by obtaining an IP PIN by accessing their Individual Online Account located online at <https://www.irs.gov/your-account>.

- (6) If the taxpayer insists on rescinding their identity theft claim after you have explained the benefits, and no other open issues exist for the tax period being rescinded:
 - a. Use IDRS Command Code REQ77 initiated from Command Code ENMOD to input a TC 972 AC 522 reflecting a Tax Administration Source Code of NOIDT and the tax year of the identity theft incident. See IRM 25.23.2-11, IMF Only TC 972 AC 522 - Reversal of TC 971 AC 522, for additional information.
 - b. Send Letter 4402C to notify the taxpayer we have closed their claim as requested using paragraph F.