EFFECTIVE DATE

(10-01-2023)

PURPOSE

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

MATERIAL CHANGES

(1) IRM 25.23.12.1 Updated the title of IRM 25.23.9 to Business Master File (BMF) Identity Theft Processing in IPU 22U1067 issued 11-04-2022. Updated IRM to include any missing titles of forms and IRM referenced in this section as of 10-01-2023.

(2) IRM 25.23.12.1.3 Updated IRM to include any missing titles of forms and IRM referenced in this section as of 10-01-2023.

(3) IRM 25.23.12.1.4 Updated the acronym for Correspondence Imaging System (CIS) to Correspondence Imaging Inventory (CII) and clarified the use of the acronym for IPSU in IPU 22U1067 issued 11-04-2022.

(4) IRM 25.23.12.1.5 Updated the title of IRM 25.23.9 to Business Master File (BMF) Identity Theft Processing in IPU 22U1067 issued 11-04-2022. Updated IRM to include any missing titles of forms and IRM referenced in this section as of 10-01-2023.

(5) IRM 25.23.12.2 Updated language above the chart to clarify the sentence. Added IRM 21.1.3.20.1 reference for IMF and BMF Oral Statement Changes to list of disclosure IRM references. Updated the website address for Department of Labor (DOL) in IPU 23U0592 issued 05-05-2023. Updated IRM to include any missing titles of forms and IRM referenced in this section as of 10-01-2023.

(6) IRM 25.23.12.2 Updated (2) language to state it is required that CSRs use the IAT Disclosure tool when conducting authentication and add MFT 32 accounts to list for additional authentication. Added a reference to IRM 21.6.2.3.3 for Telephone Inquiries Regarding Mixed Entity and Scrambled SSN Cases. Placed information previously in bullet format into If/And/Then charts to provide ease of access to information based on IRM feedback in IPU 22U1067 issued 11-04-2022.

(7) IRM 25.23.12.3(2) (b) Added an exception for disable online accounts in IPU 23U0432 issued 03-17-2023. Updated IRM to include any missing titles of forms and IRM referenced in this section as of 10-01-2023.

(8) IRM 25.23.12.4(7) Added a Reminder to include IRM references to follow for calls received from a taxpayer reporting identity theft relating to a balance due notice in IPU 23U0592 issued 05-05-2023. Updated IRM to include any missing titles of forms and IRM referenced in this section as of 10-01-2023.

(9) IRM 25.23.12.4(9) Updated processing timeframe to an average of 430 days to resolve identity theft cases due to extenuating circumstances caused by the pandemic in IPU 23U0196 issued 01-31-2023.

(10) IRM 25.23.12.4 Updated (6) Chart box 2 to include procedures for notating a dependent's account when there is no established account on TIF (entity) and you are unable to input the TC 971 AC 522 PNDCLM based on SERP Feedback 6839 in IPU 22U1216 issued 12-19-2022.

(11) IRM 25.23.12.4 Updated IRM reference provided in (4) to IRM 25.23.12.6 for IP PIN Telephone Inquiries and IRM reference in (6) for Dependent Related Identity Theft (IDT) - General to IRM 25.23.4.8.3. Updated timeframe to 360 days based on SERP Feedback 6717 and Combined (9) and (10) into one paragraph to remove redundancy in IPU 22U1067 issued 11-04-2022.

(12) IRM 25.23.12.4.1 Updated Notice CP 701C to Notice CP 01C (SP).

(13) IRM 25.23.12.4.1(1) Added a statement to refer to Non-Taxpayer Protection Program (TPP) Telephone Assistors Response to Taxpayers IRM when TPP criteria met based on SERP feedback 11340 in IPU 23U0710 issued 06-08-2023.

(14) IRM 25.23.12.4.1(3) Added a note to advise that certain disabled online accounts will not be able to order transcripts using online services in IPU 23U0432 issued 03-17-2023.

(15) IRM 25.23.12.4.1(7) Updated processing timeframe to an average of 430 days to resolve identity theft cases due to extenuating circumstances caused by the pandemic. Updated (8) Exception to provide clearer explanation and refer the reader to statement in (7) based on SERP Feedback 8487 in IPU 23U0196 issued 01-31-2023.

(16) IRM 25.23.12.4.1 Updated to include a reference for handling calls where the taxpayer states they received the Form 14611 from RAVIS in IPU 22U1216 issued 12-19-2022.

(17) IRM 25.23.12.4.1 Updated timeframe to 360 days based on SERP Feedback 6717 in IPU 22U1067 issued 11-04-2022.

(18) IRM 25.23.12.4.5 Updated to include a reference for handling calls when the taxpayer states they received the Form 14611 from RAVIS unit in IPU 22U1216 issued 12-19-2022. Updated IRM to include any missing titles of forms and IRM referenced in this section as of 10-01-2023.

(19) IRM 25.23.12.4.8 Updated IRM to include any missing titles of forms and IRM referenced in this section as of 10-01-2023.

(20) IRM 25.23.12.4.9 Updated verb tenses in language as of 10-01-2023.

(21) IRM 25.23.12.4.10 (9) Removed paragraph since any EIP 3 payment would now be claimed as the Recovery Rebate Credit (RRC) when filing the tax return.

(22) IRM 25.23.12.5(2) Updated processing timeframe to an average of 430 days to resolve identity theft cases due to extenuating circumstances caused by the pandemic in IPU 23U0196 issued 01-31-2023. Updated (2) to insert missing word “call” and any missing titles of forms and IRM referenced in this section as of 10-01-2023.

(23) IRM 25.23.12.5 Added (3) for calls where the taxpayer states they received a Form 14611 in the mail regarding the Form 4506-F they filed in IPU 22U1216 issued 12-19-2022.

(24) IRM 25.23.12.6(2) Update second bullet adding a Reminder that an IP PIN is issued to an individual’s TIN. There a spouse can’t request the re-issuance of their spouses IP PIN with authorization. Updated IRM reference from IRM 25.23.2.9.4 to IRM 25.23.2.9.4.1 and added the web address to apply for an IP PIN based on SERP feedback 10251 in IPU 23U0592 issued 05-05-2023.

(25) IRM 25.23.12.6(2) bullet 6 and 8 updated web-address for IP PIN web page on irs.gov for consistency throughout IRM 25.23 based on SERP Feedback 8814. Updated exceptions in IRM for accounts with disabled online access advising not to refer the taxpayer to online services in IPU 23U0432 issued 03-17-2023.

(26) IRM 25.23.12.6(2) Updated 8th bullet Exception to include clarification why an IP PIN for a dependent under the age of 18 could not obtained using Online services based on SERP Feedback

8105 in IPU 23U0196 issued 01-31-202 IRM 25.23.12.6.1 Updated chart in (2) Note to include a header and make 508 complaint dated 10-01-2023.

(27) IRM 25.23.12.6.1(1) Updated to include the web address to apply for an IP PIN based on SERP feedback 10183 in IPU 23U0592 issued 05-05-2023. Updated IRM to include any missing titles of forms and IRM referenced in this section as of 10-01-2023.

(28) IRM 25.23.12.6.1 Updated reminder in (2) to include accounts with disabled online access and an IRM reference. Updated (3) 2nd bullet language to reflect correct suggested language for processing IP PIN Form 15227 applications IPU 23U0432 issued 03-17-2023.

(29) IRM 25.23.12.6.1(2) Updated 7th bullet processing timeframe and provided additional language to provide caller and updated (3) 2nd bullet to provide consistent timeframe with paragraph 2 based on SERP Feedback 8294 in IPU 23U0196 issued 01-31-2023.

(30) IRM 25.23.12.6.2 Updated IRM reference from IRM 25.23.2.9.4 to IRM 25.23.2.9.4.1 in IPU 23U0592 issued 05-05-2023. Updated IRM to include any missing titles of forms and IRM referenced in this section as of 10-01-2023.

(31) IRM 25.23.12.6.2 Updated exception in (2) to include accounts with disabled online access. Added an exception to 2nd box of chart for accounts with disabled online access adjusted gross income exemption in IPU 23U0432 issued 03-17-2023.

(32) Editorial updates are made throughout the IRM to correct citations, spelling and grammar problems.

EFFECT ON OTHER DOCUMENTS

IRM 25.23.12, *Identity Protection and Victim Assistance, IMF Identity Theft Toll-Free Guidance*, effective October 1, 2022 is superseded. This IRM incorporates the following IRM Procedural Updates 22U1067 dated 11/04/2022, 22U1216 dated 12/19/2022, 23U0196 dated 01/31/2023, 23U0432 dated 03/17/2023, 23U0592 dated 05/05/2023, and 23U0710 dated 06/08/2023.

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.

Joseph Dianto
Director, Accounts Management
Wage and Investment Division

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 Responsibilities
25.23.12.1.4 Acronyms
25.23.12.1.5 Related Resources
25.23.12.2 Identity Theft Telephone General Guidance
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 Receiving Calls on Accounts Involving IPSU criteria; Identity Theft Assistance Request (ITAR)
25.23.12.4.10 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)

25.23.12.1
(10-01-2023)
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 W&I 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, Wage and Investment.

(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

(7) The IRS will not tolerate discriminatory treatment of taxpayers by its employees in any programs or activities supported by the IRS. No taxpayer should be subject to discrimination in educational programs or activities based on sex, race, color, national origin, disability, reprisal, religion, or age.

(8) If a taxpayer believes they are discriminated against on the basis of sex, race, color, national origin (including limited English proficiency), disability, reprisal, religion, or age, advise the taxpayer that they can forward an email to**EDI. Civil.Rights.Division@irs.gov*, or send a written complaint to: Internal Revenue Service, Office of Equity, Diversity, and Inclusion, CRU, 1111 Constitution, N W, Room 2413, Washington, DC 20224. A complaint form can be obtained online at *https://www.irs.gov/about-irs/your-civil-rights-are-protected*.

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
(10-01-2021)
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/taxpayer-bill-of-rights*.

(3) Policy Statement 10-1, *Assisting Taxpayers who Report they are Victims of Identity Theft*. See IRM 1.2.1.17, P–10–1 (formerly P-25-1).

25.23.12.1.3
(10-01-2023)
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) See IRM 21.1.1, Accounts Management and Compliance Services Overview. and additional information is found in IRM 1.1.13.7.3, Accounts Management (AM) and,

(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
(11-04-2022)
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
CSCO	Compliance Services Collection Operations
CSIRC	Computer Security Incident Response Center
CSR	Customer Service Representative
DV	Disclosure Verified

Acronym	Definition
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
ITAR	Identity Theft Assistance Request
ITIN	Individual Taxpayer Identification Number
MeF	Modernized e-File
MF	Master File
OAR	Operations Assistance Request
P&A Analyst	Planning and Analysis Analyst
PII	Personally Identifiable Information

Acronym	Definition
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	*Telephone Transfer Guide*
USPS	United States Postal Service
VA	Veterans Affairs

25.23.12.1.5
(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	Assistors should become acquainted with the list below of Identity Theft Victim Assistance (IDTVA) IRMs. This list is not all inclusive. • 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 ***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.
3. IRM 21	Accounts Management (AM) IRMs - Utilize and become familiar with appropriate chapters. Refer to *SERP* for access to all IRM 21 chapters.

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
(10-01-2023)
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 assistors. 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) All toll-free employees receiving calls are required to use the IAT Disclosure tool to assist callers and prevent unauthorized disclosure of taxpayer information whenever it is necessary to access a taxpayer's account. 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 do not require additional authentication unless there are other account conditions, such as an open or unresolved identity theft marker, which indicate additional authentication must be completed. See IRM 25.25.6.6, Non Taxpayer Protection Program Telephone Assistors Response to Taxpayers, when the call meets TPP criteria.

The following are additional references which discuss disclosure.

- Communication Skills, IRM 21.1.1.4
- Required Taxpayer Authentication, IRM 21.1.3.2.3
- Additional Taxpayer Authentication, IRM 21.1.3.2.4 and
- Third Party (POA/TIA/F706) Authentication, IRM 21.1.3.3
- IMF and BMF Oral Statement Address Changes IRM 21.1.3.20.1
- Telephone Inquiries Regarding Mixed Entity and Scrambled SSN Cases, IRM 21.6.2.3.3
- *TCD 0249, Communication Skills*
- Disclosure to Persons with a Material Interest, IRM 11.3.2
- 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 of a minor dependent (under 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 then follow the chart below:

If	And	Then
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,	There is a Masterfile account established for the dependent's TIN	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. Notate AMS with detailed history: • 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
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,	There is no Masterfile account established for the dependent's TIN	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. Notate AMS with detailed history: • 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.
3. 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		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. Notate AMS with detailed history: • 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,	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 referring to caller to BMF Identity theft.
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
The call is from a taxpayer reporting that they are a victim of Unemployment Identity Theft (also known as Unemployment Compensation, Insurance, or Benefits),	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: • 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. Contact Number: 1-866-487-2365 2. For Unemployment Identity Theft during the COVID-19 pandemic contact the *U.S. Department of Justice National Center for Disaster Fraud (NCDF)*. • National Center for Disaster Fund Complaint Form *https://www.justice.gov/disaster-fraud/ncdf-disaster-complaint-form* Contact Number: 1-866-720-5721

(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.

If	Then
Taxpayer prefers to access via the internet	1. Provide the IRS website, *irs.gov*, 2. Advise the taxpayer to search using key words, ″identity theft central″. If there are no further issues or questions, go to (6).

If	Then
Taxpayer states internet access is not an option, or they prefer to receive the resource information over the phone	Provide the following recommendations as applicable: 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. • 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. • Federal Trade Commission (FTC) *www.identitytheft.gov* 877-438-4338 ***Note:*** For victims needing to complete Form 14039, the FTC is currently providing a fillable Form 14039 on identitytheft.gov. This is in addition to the fillable IRS Form 14039 available on *IRS.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. • Social Security Administration (SSA) *www.ssa.gov* (type in **identity theft** in the search box) 800-772-1213

If	Then
	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. ***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. 8. Provide the caller with the identity theft toll-free number including the hours of operation located in paragraph (1) above when appropriate.

(6) 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
Dependent	Identity Theft	Refer to IRM 25.23.2.3.1, Dependent Identity Theft ***Note:*** If during a call your research determines their is an open identity theft case, refer to IRM 25.23.4.8.3, Dependent Related Identity Theft (IDT) - General.

If the Caller's inquiry is about	And	Then
IP PIN Program	• Ways to Enroll • Status of application (Form 15227, Application for an Identity Protection Personal Identification Number (IP PIN)) • Non-Receipt, lost, or misplaced	Refer to IRM 25.23.12.6, IP PIN Program Telephone Inquiries

25.23.12.3
(10-01-2023)
Non-Tax-Related Identity Theft - Self Identified

(1) Individuals experiencing non-tax-related identity theft may call the IRS for guidance.

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 the caller the program is voluntary for individuals who are not victims of tax-related identity theft and once enrolled into the IP PIN Program, there is no option for them to opt out.

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 acknowledging receipt of their IDT claim or requesting additional information.
If the caller request guidance for submitting the form either through the FTC website 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
(10-01-2023)
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, 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 25.23.12.4.10, 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 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. Enter AMS narrative by selecting **Identity Theft**; **"TP will file paper return with IDT claim"**.

Note: See IRM 25.23.2.4.4, Initial Allegations or Suspicion of Tax-Related Identity Theft - IMF Identity theft Indicators, when a taxpayer inquiries or suspects Identity Theft (IDT), for additional guidance.

(6) 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) 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.

If research confirms	Then
1. TIN matches and the dependent's TIN is being used as a primary or secondary TIN on another tax return ***Reminder:*** Do not disclose information on the return filed under the dependent's TIN.	1. Advise the taxpayer they would need to file a paper return. 2. Advise a Form 14039 can be submitted separately for/by the dependent whose TIN was used fraudulently. 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 below.

If research confirms	Then
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. ***Reminder:*** Do not disclose information on the return the dependent was claimed on.	1. Advise the taxpayer they would need to file a paper return. 2. Inquire if there is another Individual beside the parent/legal guardian who may be claiming this dependent. • If the answer is no, advise the taxpayer a Form 14039 can be submitted separately for/by the dependent whose TIN was used fraudulently. 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, provide the caller with options available for the dependent to protect their TIN by filing Form 14039. Identity Theft Affidavit, or Form 15227, Application for an Identity Protection Personal Identification Number (IP PIN). Enter AMS and select **Identity Theft**, then enter narrative **"TP will file paper return and advised of options available to protect dependent's TIN."** ***Reminder:*** IDTVA employees are not making a determination regarding which parent/legal guardian is entitled to claim and/or represent the dependent. 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 PNDCLM DEP IDT"**. 5. Continue with the call following procedures below.

For general information on Dependent Related Identity Theft (IDT), refer to IRM 25.23.4.8.3 and IRM 25.23.2.3.1, Dependent Identity Theft.

(7) 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.

(8) Advise the taxpayer there will be processing delays while the situation is resolved and they may receive correspondence requesting additional information.

(9) 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. 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 430 days to resolve 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.

(10) 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 Form 14039 and include a letter explaining their situation and provide any additional information they may think would be appropriate to substantiate their situation. Provide the taxpayer with the option of either mailing or faxing their claim. If mailing claim, provide the IRS address associated with the taxpayer's state. Refer to the *Campus Mailing Address* under the Who/Where tab on Servicewide Electronic Research Program (SERP) for Campus mailing address. 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."**
- 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.

(11) 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
(10-01-2023)
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,, 3, 4, 5, 6, 8 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) Basic and high-risk authentication must be completed using the IAT Disclosure tool for all telephone calls when the tool alerts the CSR of an IDT indicator on the account involving open, unresolved, closed, or resolved IDTVA tax related identity theft cases. See IRM 21.1.3.2.3, Required Taxpayer Authentication. 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. Fraudulent information may be 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 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 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) 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: • 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.
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 *AM Case Referral/ Reassignment Listing* 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.

(5) 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.

(6) 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 RAVIS unit, refer to IRM 25.23.12.4.5, Identity Theft - Transcript Request.

(7) 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 committed to working with victims like you to resolve tax-related identity theft cases. 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 430 days to resolve 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.*"

Note: If the time frame above has elapsed, apologize to the taxpayer and explain the processing delays due to challenges faced over the last year. 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.

(8) 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, 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 7 above for suggested timeframe statement to provide the taxpayer.

(9) After you have provided the information above to the taxpayer on their open or closed case, including sending a secure email or referral, 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."**

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 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 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
(10-01-2022)
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 un-filed 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).
3	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". Include the fax number the referral will be sent to the *"Identity Theft - Accounts Management Case Referral/ Reassignment Listing"* under the Who/Where tab on SERP ***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 reassigned to IDTVA immediately.
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
(10-01-2023)
Identity Theft - Transcript Requests

(1) Refer to IRM 21.2.3.5.8, Transcripts and Identity Theft, for guidance specific to requests involving identity theft. 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 Victims Request for Copy of Fraudulent Tax Return, **and** received the Form 14611, RAIVS/IVES IPSU, from the RAVIS unit, also refer to IRM IRM 21.3.6.4.3.2, Return Copy Procedures and Identity Theft for additional guidance.

25.23.12.4.5.1
(10-01-2022)
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 researching.

(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 25.23.2-16, 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
(10-01-2021)
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) and (8).

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
(10-01-2023)
Receiving Calls on Accounts Involving IPSU criteria; Identity Theft Assistance Request (ITAR)

(1) Effective October 1, 2022 the Identity Theft Assistance Request (ITAR) inventory program is obsolete. AM IDTVA will no longer be accepting ITAR e4442s. See IRM 21.3.5.4.1, When to Prepare a Referral, to determine if an e4442 is required based on a specific topic.

25.23.12.4.10
(10-01-2023)
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(4), Identity Theft Telephone General Guidance.

(6) 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, 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 account research determines no EIPs were issued due to ineligibility, explain to the taxpayer how EIPs are determined. Example: Reason Code (RC) 201 No payment due to the taxpayer being claimed on another return. See IRM 25.23.4.20.1, Economic Impact Payment (EIP) - Account Research. If the taxpayer insist, after the explanation, that a fraud was committed using their personally identifiable information without their authority; refer to IRM 25.23.12.2 (4), Identity Theft Telephone General Guidance. Provide guidance to the taxpayer including actions to take to protect their identity.

(7) If your research confirms the taxpayer's Economic Impact Payment (EIP) was issued to the taxpayer's bank account or mailed to the taxpayer's address of record as a paper check and the taxpayer did not receive it, follow procedures in IRM 21.4.2.4, Refund Trace Actions, to locate and trace a lost, stolen, or misplaced payment. If you identify a TC 971 AC 199 with a miscellaneous field "BFS DEBIT" dated May 22, 2020, "BFS DEBIT II" dated January 6, 2021, or **BFS DEBIT 2021A** dated March 26, 2021 on the entity module, this indicates a Pre-paid debit card(s) was issued for the refund(s). The EIP card is sponsored by the Bureau of Fiscal Service (BFS), managed by Money Network Financial, LLC, and issued by Treasury's financial agent, Metabank. Do not initiate a refund trace on debit card. If the credit has not been returned to the account (TC 841 or TC 740), advise the taxpayer to contact Metabank at 800-240-8100 (select language, then option 2 for main menu, then enter the last six digits of the Social Security number of the person who is listed first on the tax return, or at eipcard.com. For more information see IRM 21.6.3.4.2.13.2, Economic Impact Payments – Refund Inquiries and follow any procedures that may apply. For all other refund inquiries such as returned refunds, family disputes, or erroneous refund, etc., see the appropriate section of IRM 21.4, Refund Inquiries.

(8) Research to determine if the taxpayer's account has a TC 971 AC 199 miscellaneous field that shows a bank account number followed by the letters "EF" on the taxpayer's entity and the taxpayer claims that they did not file a current year return, use any *IRS.GOV* applications to enter their information, or provide the federal government with any direct deposit information to receive benefits. If a TC 971 AC 199 miscellaneous field that shows a bank account number followed by the letters "EF" and the taxpayer claims they never provided any information using the IRS.gov applications or received EIP payments, advise the taxpayer to submit an identity theft claim using Form 14039,

Identity Theft Affidavit. 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
(10-01-2023)
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. Ask if the requestor 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
  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 430 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) 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
(10-01-2023)
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. Once a taxpayer is enrolled into the IP PIN Program, there is no option for the taxpayer to opt out of 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.

2. Applying Online using Get an IP PIN Tool	Online tool that allows taxpayers to enroll in (opt-in) the IP PIN Program or display their IP PIN if already enrolled. See IRM 25.23.2.9.1.2, Get an IP PIN Application Online Available for Taxpayers to Opt-In to the IP PIN Program, for more information. ***Note:*** Inform the taxpayer this is the quickest way to obtain an IP PIN at www.irs.gov/ippin and will be able to obtain their IP PIN and use it immediately.
3. 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), 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, employees will:

- 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 questions.
- 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.

  Reminder: An IP PIN is issued for an individual's TIN. Joint taxpayers may only request for their IP PIN to be re-issued. If they are calling to obtain their spouse's IP PIN they must follow procedures in IRM 21.1.3.3, Third Party (POA/TIA/F706) Authentication.
- 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. Advise the taxpayer they may also try to obtain their IP PIN at *www.irs.gov/ippin* to avoid mailing delays.

#
#
#

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 return processing their return and issuance of any refund that may be due.
- Educate the taxpayer, that in the future, they can retrieve their original IP PIN through *www.irs.gov/ippin* when Modernized Electronic Filing (MEF) is available.

#
#
#
#
#
#
#
#
#

- 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 to receive their CP 01A notice) and 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 requires the submission of a Form 8822, Change of Address. This should be completed using the dependent's TIN and name so there is no interruption in receiving their yearly CP 01A notice.

25.23.12.6.1
(10-01-2023)
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. The fastest way for an individual to enroll in the IP PIN Program is using the Get an IP PIN Application online at www.irs.gov/ippin. 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 taxpayers or they may call to request a copy at 800-829-3676. Information is also available on line: *IRS Forms*.
- 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*. Advise the taxpayer to search using key words “IP PIN” or “Form 15227” for a list of options available to apply for an IP PIN including the Form 15227 IP PIN paper process instructions.
- 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 the form can be mailed or faxed (not both) and then 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**
If submitting Form 15227 by mail: Department of the Treasury, IRS Fresno, CA 93888-0025 If using a private delivery service (FedEx or UPS), provide the following street address: Department of the Treasury, IRS 3211 S Northpointe Dr. Fresno, CA 93725	If submitting Form 15227 by fax: Include a cover sheet marked ‘Confidential’ Fax to the toll-free number 855-807-5720

- 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

430 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 mailed/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 430 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.
- 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 8812 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 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.

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 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
(10-01-2023)
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.)	• 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.

If there is an Open	Then
IDTX control	• 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	• 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 DDKBD. 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	• 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
No	• Advise them the "Get an IP PIN" 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 $ 73,000 (any filing status other than married filing joint) or $ 146,000 (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
Yes, but attempts to use online process ("Get an IP PIN" application tool) was unsuccessful ***Reminder:*** If the individual experienced difficulty using Secure Access e-Authentication or is unable to verify their identity using the Get an IP PIN Online Application, continue with providing alternative IP PIN Program options. IRM 25.23.2.9.1, Participating in the IP PIN Program.	• Research the individual's latest tax return on file. Determine if their adjusted gross income is equal to or below $ 73,000 (any filing status other than married filing joint) or $ 146,000 (filing status of married filing joint), if yes then recommend they file Form 15227, Application for an Identity Protection Personal Identification Number (IP PIN). • If the individual's adjusted gross income on their federal tax return is above $ 73,000 (any filing status other than married filing joint) or $ 146,000 (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
Yes, they filed a Form 15227 and received a Letter 4403C advising them we were unable to process their IP PIN request	• 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 an IDTX closed 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. ***Note:*** Visiting a TAC for an IP PIN Appointment is only available for applicants who reside in the US.

(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
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:	• A driver's license • State identification card • Passport ***Reminder:*** Any current US federal or state government issued identification presented **MUST** be signed by the issuing agency and/or the individual where appropriate.
They **must** provide **at least one additional** form of identification such as:	• 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 ***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.

Who must present forms of Identification/Documentation	Identification/Documentation Required for IP PIN Application TAC Appointment

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)
	• Birth Certificate (Requires Name at Birth, Date of Birth, and City of Birth)
	• Bank Statements
	• Social Security card
	• Student Records (grade/ high school/college)
	Note: Accept school records from the last year completed plus one other item from the list.
	• 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:
	  • 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.