



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

25.23.2

AUGUST 26, 2024

EFFECTIVE DATE

(10-01-2024)

PURPOSE

- (1) This transmits revised IRM 25.23.2, Identity Protection and Victim Assistance - General Case Processing.

MATERIAL CHANGES

- (1) IRM 25.23.2.2.1(3), Updated to include option and link to submit Form 14039 online via www.irs.gov. IPU 24U0199 issued 02-02-2024.
- (2) IRM 25.23.2.2.3 - Updated IDT processing timeframe from 430 days to 480 days throughout the IRM. In paragraph 5, removed the last column in the table and added the content as a **Note** to ensure 508 compliance. IPU 23U0987 issued 10-02-2023.
- (3) IRM 25.23.2.2.3, Updated IDT processing timeframe from 650 days to 640 days. IPU 24U0844 issued 07-16-2024
- (4) IRM 25.23.2.2.3, Updated IDT processing timeframe from 480 days to 650 days. IPU 24U0199 issued 02-02-2024.
- (5) IRM 25.23.2.3, Added clarification for situations when the IDT victim is the secondary taxpayer.
- (6) IRM 25.23.2.4.5(6) - Added a link to IRM 25.23.2.6(5), to reduce confusion and emphasize that “NOIDT” scenarios are resolved differently in regard to missing TC 971 AC 522s. IPU 23U0987 issued 10-02-2023.
- (7) IRM 25.23.2.3(1)(b), Updated Note to include option and link to submit Form 14039 online via www.irs.gov. IPU 24U0199 issued 02-02-2024.
- (8) IRM 25.23.2.3.1(6), Removed the dashes from “WI-ITVAA-OTHER” and “WI-ITVAC-OTHER” to prevent confusion. IPU 24U0199 issued 02-02-2024.
- (9) IRM 25.23.2.3.8.1(2), Added an exception for IDTVA employees to direct them to Exhibit 25.23.4-21. IPU 24U0199 issued 02-02-2024.
- (10) IRM 25.23.2.3.8.1(2) Clarified that the exception is for reversals of IDT indicators with a secondary date older than 7 years. IPU 24U0770 issued 06-17-2024.
- (11) IRM 25.23.2.3.10(2), Corrected the paragraph selection and additional verbiage for Letter 4402C.
- (12) IRM 25.23.2.4.4, Added clarification on processing claims when the IDT victim is the secondary taxpayer.
- (13) IRM 25.23.2.6.2 - (3)(a) Removed verbiage regarding removal from IP PIN population.
- (14) IRM 25.23.2.6.3 - (3) Removed reminder regarding removal from IP PIN population.
- (15) IRM 25.23.2.6.4 (1) (e) Removed reminder regarding removal from IP PIN population.

- (16) IRM 25.23.2.7.2.1(2) Reworded the REMINDER for clarity and added link to IRM 25.25.6.6.6. Added a link to IRM 10.10.3.3.6 in the first "Then" box of the table in paragraph 3. IPU 24U0770 issued 06-17-2024.
- (17) IRM 25.23.2.8, added description of AC 528. Removed verbiage that taxpayer cannot be removed from the IP PIN population.
- (18) IRM 25.23.2.8.1.1(4), Corrected the Example to indicate a TC 971 AC 504 with MISC "EMPL-M" should be used since more than one tax year is impacted. IPU 24U0199 issued 02-02-2024.
- (19) IRM 25.23.2.8.4(6), Corrected IRM reference from IRM 21.6.6.2.20.3 to IRM 21.6.6.2.21.3. IPU 24U0199 issued 02-02-2024.
- (20) IRM 25.23.2.8.4.2(1), Corrected IRM reference from IRM 21.6.6.2.20.1 to IRM 21.6.6.2.21.1. IPU 24U0199 issued 02-02-2024.
- (21) IRM 25.23.2.8.5 - (5) (i) Chart 1st row - removed Reminder regarding removal from IP PIN population.
- (22) IRM 25.23.2.8.7, Added new IRM subsection 25.23.2.8.7 will address TC 971 AC 528. The IRM has been re-numbered to accommodate new subsection.
- (23) IRM 25.23.2.8.9.1(5), Corrected the paragraphs needed for Letter 4674C.
- (24) IRM 25.23.2.9(1), Clarified that IP PINs are used to protect both SSNs and ITINs. Removed (6) regarding removal from IP PIN population.
- (25) IRM 25.23.2.9.1, Added new paragraph 2 which explains that individuals who are not victims of identity theft and voluntarily opted in to the IP PIN program now have the ability to opt out. IPU 24U0844 issued 07-16-2024
- (26) IRM 25.23.2.9.1 Changed "Get an IP PIN application" references to "Individual Online Account." IPU 24U0770 issued 06-17-2024.
- (27) IRM 25.23.2.9.1(1), Corrected the IRM reference from IRM 25.23.3.2.8, to IRM 25.23.3.2.7 in the third box of the table. IPU 24U0199 issued 02-02-2024.
- (28) IRM 25.23.2.9.1.2(2), Added information which explains that individuals who are not victims of identity theft and voluntarily opted in to the IP PIN program now have the ability to opt out. IPU 24U0844 issued 07-16-2024
- (29) IRM 25.23.2.9.1.2 Updated IRM title to, "Opting in to the IP PIN Program through the Individual Online Account." Removed outdated information in paragraph 1 and changed "Get an IP PIN application" references to "Individual Online Account. IPU 24U0770 issued 06-17-2024."
- (30) IRM 25.23.2.9.3 IRM was re-worded for clarity and to include references to the Individual Online Account. IPU 24U0770 issued 06-17-2024.
- (31) IRM 25.23.2.9.3(3), Added an Exception to show that a TC 971 AC 528 will bypass the non-filer suppression criteria.
- (32) IRM 25.23.2.9.4 Changed "Get an IP PIN application" reference to "Individual Online Account." Reworded third bullet in paragraph 3 for clarity. IPU 24U0770 issued 06-17-2024.
- (33) IRM 25.23.2.9.4.1 Changed "Get an IP PIN application" reference to "Individual Online Account." Added instructions to advise taxpayers of the self-help methods to retrieve IP PINs if disclosure is not

passed. Changed “dependents” to “minor dependents” where applicable. Added new paragraph 9 to remind taxpayers to file Form 8822 if they change their address before the upcoming filing season. IPU 24U0770 issued 06-17-2024.

- (34) Exhibit 25.23.2-2(5), Corrected the definition of “OTHER” to ensure consistency with related IRMs.
- (35) Exhibit 25.23.2-2(13), Removed “REFCCA” and “ICMCCA” from the ITVAC table until a programming error is resolved. IPU 24U0199 issued 02-02-2024.
- (36) IRM 25.23.2, Revised throughout to update organizational title “Wage and Investment” to “Taxpayer Services”. Also updated “IVO” to “RIVO”.

EFFECT ON OTHER DOCUMENTS

IRM 25.23.2 dated October 1, 2023, is superseded and includes the following IRM Procedural Updates: IPU 23U0987 issued 10-02-2023, IPU 24U0199 issued 02-02-2024, IPU 24U0770 issued 06-17-2024 and IPU 24U0844 issued 07-16-2024

AUDIENCE

The provisions in this manual apply to all divisions, functional units, employees and contractors within the IRS working identity theft cases.

Lucinda Comegys
Director, Accounts Management
Taxpayer Services Division

25.23.2

Identity Protection and Victim Assistance - General Case Processing

Table of Contents

25.23.2.1 Program, Scope and Objectives

25.23.2.1.1 Acronyms, Definitions and Background of the Identity Protection Program

25.23.2.1.2 Related Internal Revenue Manuals (IRM) and other Reference Materials

25.23.2.2 Identity Theft - Overview

25.23.2.2.1 Taxpayer Interaction

25.23.2.2.2 Priority Handling of Identity Theft Cases

25.23.2.2.3 IDT Case Processing Time Frames

25.23.2.3 Identity Theft Claims – General Guidelines

25.23.2.3.1 Dependent Identity Theft

25.23.2.3.2 Assessing the Scope of the Taxpayer's Issues

25.23.2.3.2.1 Addressing All Taxpayer Issues

25.23.2.3.3 Identity Theft Case Controls

25.23.2.3.4 Required Case and History Notes

25.23.2.3.5 Identity Theft Research

25.23.2.3.5.1 Economic Impact Payments – General Information

25.23.2.3.6 When to Request Additional Information to Support an Allegation of Identity Theft

25.23.2.3.7 When to Update the Victim's Address

25.23.2.3.8 Marking Taxpayer Accounts When Accepting Identity Theft Claims

25.23.2.3.8.1 Command Code REQ77 Secondary Date and Old Case Year Issue

25.23.2.3.9 Taxpayer Advocate Service

25.23.2.3.10 Electronic Products Service and Support (EPSS) Disabled Accounts

25.23.2.4 IDT Indicators – Tax Related

25.23.2.4.1 Tracking and Reporting Identity Theft Cases - Identity Theft Indicators

25.23.2.4.2 Tracking IMF Tax-Related Identity Theft Inventory

25.23.2.4.3 Tracking Individual Taxpayers Reporting to be Victims of Business-Related Identity Theft

25.23.2.4.4 Initial Allegation or Suspicion of Tax-Related Identity Theft - IMF Identity Theft Indicators

25.23.2.4.4.1 IMF Identity Theft- Taxpayer Initiated Allegations of Identity Theft - TC 971 AC 522

25.23.2.4.4.2 Mass Input of Identity Theft Tracking Indicators

25.23.2.4.5 IRS Initiated Suspicion of Identity Theft - TC 971 AC 522 IRSID

25.23.2.5 Statute Protection

25.23.2.5.1 Statute Protection - Single Return

25.23.2.5.2 Statute Protection - Multiple Returns

25.23.2.5.3 Statute Protection - Multiple Returns and MFT 32

25.23.2.5.4 Barred Statutes

25.23.2.6 Closing Identity Theft Issues

- 25.23.2.6.1 Closing Taxpayer Initiated Identity Theft Affecting Tax Administration - TC 971 AC 501
 - 25.23.2.6.1.1 Systemic Actions Taken After TC 971 AC 501 Placed on Account
- 25.23.2.6.2 Manually Reversing TC 971 AC 501
- 25.23.2.6.3 Closing IRS Determined Identity Theft Affecting Tax Administration - TC 971 AC 506
- 25.23.2.6.4 Manually Reversing TC 971 AC 506
- 25.23.2.6.5 Closing Identity Theft Cases with Tax Delinquency Inquiries (TDI)
- 25.23.2.6.6 Reversing Unsupported Allegations of Identity Theft
 - 25.23.2.6.6.1 No Reply – TC 972 AC 522 NORPLY
 - 25.23.2.6.6.2 No Identity Theft (NOIDT) Determinations – TC 972 AC 522 NOIDT
- 25.23.2.6.7 TC 971 AC 522 PNDCLM/UNWORK/IRSID - Incorrect Tax Year
- 25.23.2.7 IMF Identity Theft Worked by Functions Outside Accounts Management IDTVA
 - 25.23.2.7.1 Identity Theft Identified by Criminal Investigation
 - 25.23.2.7.2 Return Integrity and Compliance Services (RICS). Identity Theft Identified by: Return Integrity & Verification Operations (RIVO) and the Taxpayer Protection Program (TPP) Excludes Former WI Compliance Exam Operations
 - 25.23.2.7.2.1 Returns Selected by Identity Theft Filters - Taxpayers Visiting the TAC
 - 25.23.2.7.2.2 MFT 32 - Overview
 - 25.23.2.7.3 Identity Theft Identified by Submission Processing
- 25.23.2.8 Miscellaneous Identity Theft Indicators
 - 25.23.2.8.1 IMF TC 971 AC 504
 - 25.23.2.8.1.1 TC 971 AC 504 with Miscellaneous Field Codes ACCT, ACCT-M, BOTH, BOTH-M, EMPL, EMPL-M, ICMCCA, NKI or NKI-M
 - 25.23.2.8.1.2 TC 971 AC 504 - Miscellaneous Field Code SPCL1, SPCL2, RPM1, RPM2, RPM3, RPM4, and EAFail
 - 25.23.2.8.1.3 IMF Only - Manually Reversing TC 971 AC 504
 - 25.23.2.8.2 IRS Data Breaches- TC 971 AC 505
 - 25.23.2.8.4 Locking Decedent Accounts - TC 971 AC 524
 - 25.23.2.8.4.1 Manually Reversing TC 971 AC 524 - Date of Death Present on Command Code INOLES
 - 25.23.2.8.4.2 Manually Reversing TC 971 AC 524 - No Date of Death Present on Command Code INOLES
 - 25.23.2.8.5 Employment-related Identity Theft – TC 971 AC 525
 - 25.23.2.8.6.1.2 Resolving Non-Tax Related Affected Accounts with TC 971 AC 527
 - 25.23.2.8.7 TC 971 AC 528

#

#

#

#

#

#

- 25.23.2.8.9 TC 971 AC 123 PREPARER CONTACT
 - 25.23.2.8.9.1 TC 971 AC 123 PREPARER CONTACT - Taxpayer Contact
- 25.23.2.9 Identity Protection Personal Identification Number (IP PIN)
 - 25.23.2.9.1 Participating in the IP PIN Program
 - 25.23.2.9.1.1 Automatic Enrollment in the IP PIN Program
 - 25.23.2.9.1.2 Opting into the IP PIN Program through the Individual Online Account
 - 25.23.2.9.1.3 IP PIN TAC Appointment Procedures
 - 25.23.2.9.1.3.1 IP PIN TAC Procedures- (TAC Employees Only)
 - 25.23.2.9.2 Identifying If a Taxpayer has an IP PIN Requirement
 - 25.23.2.9.3 Receiving and/or Retrieving your Annual IP PIN
 - 25.23.2.9.4 Lost, Misplaced or Non-Receipt of IP PIN Overview
 - 25.23.2.9.4.1 Lost, Misplaced or Non-Receipt of IP PIN
 - 25.23.2.9.5 Filing Returns with an IP PIN
- 25.23.2.10 Get Transcript Breach
- 25.23.2.11 Get an Electronic Filing PIN Incident
- 25.23.2.12 Free Application for Federal Student Aid (FAFSA) Breach
 - 25.23.2.12.1 FAFSA Breach-CP302
- 25.23.2.13 Breach Numbers CR20170421067 and LR20170421067
- 25.23.2.14 Form 8821 Breach
- 25.23.2.15 Identity Theft Liaison Responsibilities
 - 25.23.2.15.1 Functional Responsibilities in Receipt of Global Review (GRVW) Referrals

Exhibits

- 25.23.2-1 Acronyms and Definitions
- 25.23.2-2 IMF Only TC 971 AC 501 — Taxpayer Initiated Identity Theft Case Closure (Tax-Related) - TC 971 AC 501
- 25.23.2-4 IMF Only TC 971 AC 504
- 25.23.2-5 IMF Only TC 972 AC 504 — Reversal of TC 971 AC 504
- 25.23.2-6 IMF Only TC 971 AC 505 — IRS Data Breaches
- 25.23.2-7 IMF Only TC 972 AC 505 — Reversal of TC 971 AC 505
- 25.23.2-8 IMF Only TC 971 AC 506 — IRS Determined Tax-Related Identity Theft Case Closure
- 25.23.2-9 IMF Only TC 972 AC 506 Tax-Related, Reversal of Identity Theft Case Closure, IRS Identified
- 25.23.2-10 IMF Only TC 971 AC 522 Tax-Related Identity Theft, Case Status (Initial Claim/Suspicion)
- 25.23.2-11 IMF Only TC 972 AC 522 - Reversal of TC 971 AC 522
- 25.23.2-12 TC 971 AC 523 – Reserved

#

#

-
- 25.23.2-14 TC 971 AC 524 – Locking SSNs - Applies to IMF Accounts Only
- 25.23.2-15 TC 972 AC 524 – Reversal of TC 971 AC 524
- 25.23.2-16 IDTVA IDRS Category Controls by Function

25.23.2.1
(09-15-2020)
Program, Scope and Objectives

- (1) **Purpose:** This manual defines the mission, objectives, and governance structure of the Identity Protection and Victim Assistance Program. It provides the organizational framework for carrying out specific policies and procedures aimed at preventing identity theft, protecting taxpayers and helping victims of identity theft.
- (2) **Audience:** The primary users of the IRM are anyone working identity theft inventory and helping victims of identity theft.
- (3) **Policy Owner:** The Director of Accounts Management.
- (4) **Program Owner** Accounts Management - Identity Protection Strategy and Oversight (IPSO).
- (5) **Primary Stakeholders** Taxpayers who are victims of identity theft and the employees working to assist them.
- (6) **Program Goals:**
 - The development of short-term and long-term remedies to protect taxpayer information and make the experience of those who are already victims faster and more efficient.
 - The development of servicewide policy, procedures, and guidelines for the priority of recognizing, marking and acknowledging individual taxpayer claims involving identity theft.
 - Support of IPSO activities within the scope of programs associated with identity protection.

25.23.2.1.1
(09-06-2023)
Acronyms, Definitions and Background of the Identity Protection Program

- (1) For a list of acronyms, see Exhibit 25.23.2-1 , *Acronyms and Definitions*.
- (2) For terms and definitions see IRM 25.23.1.1.2 , *Key Definitions*, and Exhibit 25.23.1-1 , *Glossary of Identity Protection Terms and Definitions*.
- (3) For program background, see IRM 25.23.1.1.1 , *Background of the Identity Protection Program*.

25.23.2.1.2
(09-06-2023)
Related Internal Revenue Manuals (IRM) and other Reference Materials

- (1) Throughout IRM 25.23.2, *Identity Protection and Victim Assistance - General Case Processing*, there are links/references to other IRMs for handling program specific issues.
- (2) Employees are responsible for familiarizing themselves with and utilizing all linked/referenced IRMs, as appropriate. This includes, but is not limited to sections, within the following:
 - IRM 2, *Information Technology*
 - IRM 3, *Submission Processing*
 - IRM 4, *Examining Process*
 - IRM 5, *Collecting Process*
 - IRM 10.5 , *Privacy and Information Protection*
 - IRM 11.3, *Disclosure of Official Information*
 - IRM 13, *Taxpayer Advocate Service*
 - IRM 20, *Penalty and Interest*
 - IRM 21, *Customer Account Services*
 - IRM 25, *Special Topics*

25.23 Identity Protection and Victim Assistance

In addition, this IRM links to these IDTVA function specific IRMs:

- IRM 25.23.1, *Identity Protection and Victim Assistance - Policy Guidance*
- 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*
- IRM 25.23.10, *Compliance Identity Theft Case Processing*
- IRM 25.23.11, *Business Master File (BMF) Identity Theft Procedures for Accounts Management*
- IRM 25.23.12, *IMF Identity Theft Toll-Free Guidance*
- IRM 25.23.13, *Income Related Identity Theft*
- IRM 25.24.1, *Return Preparer Misconduct Victim Assistance - General Overview*
- IRM 25.24.2, *Return Preparer Misconduct Victim Assistance Specialized Accounts Management Processing*

25.23.2.2 (10-01-2018) **Identity Theft - Overview**

- (1) The following subsections give a brief overview for communication with and casework for victims of identity theft.

25.23.2.2.1 (02-02-2024) **Taxpayer Interaction**

- (1) All taxpayers deserve and expect courteous service. Taxpayers who have experienced identity theft are already victims, either emotionally or financially. Internal Revenue Service (IRS) employees need to be aware of the impact of being an identity theft victim and handle the contact with an additional level of sensitivity and understanding. You must also guard against unauthorized disclosures and verify you are talking to the taxpayer or their authorized representative.

Note: As stated in the *Taxpayer Bill of Rights*, taxpayers have the right to quality service, which means that they have the right to receive prompt, courteous and professional assistance in their dealings with the IRS, to be spoken to in a way they can easily understand, to receive clear and easily understandable communications from the IRS, and to speak to a supervisor about inadequate service.

- (2) Victims may suffer more than the loss of funds and ruination of their credit rating. Among other costs, victims may be subjected to potential loss of opportunities, such as those associated with employment and housing.
- (3) Educate the victims about the Federal Trade Commission's website at <https://www.identitytheft.gov>. The FTC site provides information how to file a claim electronically or by mail. The FTC states that it **IS** a law enforcement agency and reporting through them removes the need to file a police report to verify the claim. This is the "one-stop-resource for victims of identity theft". For more information see IRM 25.23.12.2, *Identity Theft Telephone General Guidance*. In addition to informing the victim of the FTC information, advise them to:
 - File Form 14039, Identity Theft Affidavit, with the IRS if the identity theft affects tax administration.
 - If the taxpayer requested protection of their tax account and no tax-related identity theft has occurred, advise the taxpayer the best way to protect their TIN (SSN/ITIN) is by participating in the IP PIN program. Provide the caller with information on opting-in or applying to participate

in the IP PIN Program. See IRM 25.23.12.3, *Non-Tax Related Identity Theft - Self Identified*, for additional information.

Reminder: If the taxpayer previously submitted a Form 14039 to the IRS for a tax-related issue, there's no need to submit another Form 14039 unless it is submitted as the result of a separate and different incident that will change the treatment of the case (i.e., non-tax to tax related).

Reminder: Form 14039, Identity Theft Affidavit, can be mailed, faxed or sent electronically. The IRS is currently providing an on-line Form 14039 at <https://apps.irs.gov/app/digital-mailroom/dmaf/f14039/> on <https://www.irs.gov/>. This is in addition to the fillable FTC Form 14039 available at <https://www.identitytheft.gov/>. Unsigned forms are acceptable.

- Review Publication 5027, Identity Theft Information for Taxpayers.
- Review the IRS website at *Identity Theft Central*.
- Check with their state tax agency to see if there are additional steps they could take at the state level.

For additional information, see IRM 25.23.12, *IMF Identity Theft Toll-Free Guidance*.

- (4) Taxpayers meeting Taxpayer Advocate Service (TAS) Criteria 1-4 (economic burden) will be referred to TAS, see IRM 21.1.3.18, *Taxpayer Advocate Service (TAS) Guidelines*.

Caution: If IRS can provide relief or take a substantive action towards providing relief within 24 hours, do not send the case to TAS, unless the taxpayer requests TAS assistance and the case meets TAS criteria.

25.23.2.2.2 (10-01-2022) Priority Handling of Identity Theft Cases

- (1) All cases involving identity theft will receive priority treatment. **This includes functions not located within the IDTVA framework.** Refer to IRM 25.23.1.2, *Taxpayer Services - Accounts Management - Identity Protection Strategy and Oversight (IPSO)*, for additional information.
- (2) The following forms will be treated as priority:
- Form 14039, Identity Theft Affidavit
 - Form 14039(SP), Identity Theft Affidavit (Spanish)
 - Form 14027-B, Identity Theft Case Referral
 - Form 4506-F, Request for Fraudulent Return
 - Form 15227(EN-SP), Application for an IP PIN

25.23.2.2.3 (07-16-2024) IDT Case Processing Time Frames

- (1) To provide taxpayers who are victims of identity theft with a realistic expectation of the timeframe for resolution of their cases, advise them that generally cases are resolved within 120 days; however, due to extenuating circumstances caused by the pandemic, our identity theft inventories have increased dramatically and on average it is taking us 640 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 backlog.
- (2) The timeframe will generally be calculated from the received date of the taxpayer's identity theft claim. Thorough IDRS/AMS research is required to

25.23 Identity Protection and Victim Assistance

identify the received date of the taxpayer's valid claim (TPRQ/SPC1, IDT1/IDS1, TPPI, etc.) to begin calculating the timeframe for your case.

Note: For CP36I cases, the timeframe begins with the issuance of the CP01S (located on TXMOD TC 971 AC 804 MISC "CP001S-SPC8").

IF	THEN
Claim is not available for review or is missing a date stamp	Begin the calculation from the earliest issuance date of the: <ul style="list-style-type: none"> • Letter 5073C • Notice CP 01S or Notice CP 701S
CP 36I cases	The timeframe begins with the issuance of the CP01S
IRS identified ID theft	The timeframe begins on the date the case was recognized as identity theft (case controlled or converted to an identity theft category code)

Reminder: A TC 971 AC 522 with one of the following Tax Administration Source Codes may be present when the taxpayer initiates a claim alleging identity theft for a specific tax year. See IRM 25.23.2.3 , *Identity Theft Claims - General Guidelines*.

Tax Administration Source Codes
UNWORK
INCOME
INCMUL
MULTFL
NOFR
OTHER

(3) Use the following table to calculate the identity theft timeframe:

If the taxpayer	Then the identity theft timeframe must be calculated from:
Has filed a loose Form 14039, Identity Theft Affidavit, (or other acceptable documentation as defined in IRM 25.23.2.3, <i>Identity Theft Claims - General Guidelines</i>). Note: To determine if the taxpayer filed a loose claim, generally there will be either an open IDT1/IDS1, IDT4, IDT9/IDS9, or IDs, etc. control. If available, view the scanned or attached documents with the related CII case to determine if the case involves the filing of identity theft information.	The IDRS received date of the control associated with the Form 14039 (or other acceptable documentation as defined in IRM 25.23.2.3, <i>Identity Theft Claims - General Guidelines</i>)
Attached the Form 14039 to their tax return that resulted in a CP 36I.	The timeframe begins with the issuance of the CP01S
Submitted information to a function other than Accounts Management (ex: TPPI).	The IDRS received date of the control associated with the information (ex: TPPI).

- (4) Be empathetic to the taxpayer's issue. Assure the taxpayer that the IRS is firmly 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 correct determination for case resolution.
- (5) Apologize to the taxpayer for the length of time required to resolve their issue. Explain that identity theft is complex in nature and constantly changing.
Suggested language is:

We apologize for the length of time it is taking to resolve your case. Identity theft is a challenging and ever-changing issue. 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 650 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.

25.23 Identity Protection and Victim Assistance

If the taxpayer	Then state
Is claiming to be experiencing an economic burden/hardship (TAS Criteria 1-4).	You will be referring them to the Taxpayer Advocate Service for immediate attention. See IRM 21.1.3.18, <i>Taxpayer Advocate Service (TAS) Guidelines</i> .
Is waiting to hear about an identity theft related tax issue previously submitted.	Please allow us more time to properly address your concerns. Due to extenuating circumstances caused by the pandemic our identity theft inventories have increased dramatically and on average it is taking us 650 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.
Called before and a shorter timeframe was communicated to them.	Please allow us more time to properly address your concerns. Due to extenuating circumstances caused by the pandemic our identity theft inventories have increased dramatically and on average it is taking us 650 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.
Inquires about the upcoming filing season.	They must continue to file their tax return while their identity theft claim is under review. They may be able to e-file or may have to file a paper tax return as an alternative. Advise there may be delays in the processing timeframe.
Is not aware of the identity theft guidance available.	General identity theft guidance in IRM 25.23.12.2, <i>Identity Theft Telephone General Guidance</i> .

Note: If necessary, close your explanation with: “Again, I apologize for the inconvenience and ask for your patience as we work to resolve your identity theft case.”

25.23.2.3 (10-01-2024) Identity Theft Claims – General Guidelines

- (1) Form 14039, Identity Theft Affidavit, is used to report both tax-related and non-tax-related identity theft issues. The affidavit is also available in Spanish; Form 14039 SP. Form 14039 retention will follow case retention procedures of the function working the case.
 - a. Advise taxpayers to submit a claim using Form 14039 when they allege they are victims of tax-related identity theft. If the taxpayer files/will file as MFJ, explain that the Form 14039 be filed for the individual who is impacted by identity theft regardless of whether that individual is the

primary or secondary taxpayer on a joint return; if both the primary and secondary taxpayers are impacted, a Form 14039 should be filed for each TIN.

- b. The taxpayer is welcome to file a Form 14039 for non-tax related issues. If a taxpayer requests that their SSN be marked, red flagged/protected, etc., then provide guidance for submitting the form online either through <https://apps.irs.gov/app/digital-mailroom/dmaf/f14039/> on www.irs.gov, the FTC website or by paper. For additional information, see IRM 25.23.2.2.1, *Taxpayer Interaction*.

Note: In situations where the taxpayer initially asserts identity theft and provides an IDT claim and/or additional information at the same time, mark the account with one TC 971 AC 522 reflecting receipt of the claim using the Tax Administration Source Code UNWORK.

- (2) Identity theft claims and/or additional information can be accepted from the taxpayer, third party (e.g., taxpayer reports for their spouse), or someone who has power of attorney for the taxpayer (e.g., Form 2848, Power of Attorney and Declaration of Representative).
- (3) Taxpayer claims may cover more than one tax year. The taxpayer does not need to submit a separate claim for each year affected by identity theft.
- (4) Form 14039 can be submitted by either mail or fax following the instructions provided on the second page of the Form 14039. For example:

If the taxpayer alleges tax-related identity theft AND	Then advise the taxpayer to complete Form 14039 AND
The taxpayer was unable to file his/her return electronically because the primary and/or secondary SSN was misused	Mail Form 14039 to: Department of the Treasury Internal Revenue Service Fresno, CA 93888-0025
The taxpayer already filed a paper return	Submit to the IRS location where he/she normally files.
The taxpayer is responding to a letter or notice he/she received	Submit with a copy of the notice or letter to the address contained in the notice or letter.

Note: Form 14039 no longer requires a signature or the submission of additional information/documentation.

- (5) The individual receiving an identity theft claim as defined in Exhibit 25.23.1-1, *Glossary of Identity Protection Terms and Definitions*, will acknowledge receipt within 30 days of the IRS received date.

Exception: IDTVA will acknowledge IDT Claims received in Compliance within 30 days of receipt from Compliance.

#

25.23 Identity Protection and Victim Assistance

Exception: No acknowledgement letter is necessary if you will resolve the case within 30 days. The closing letter will serve as an acknowledgement in that case. If TC 971 AC 501 is used to generate closing letter, leave a case note to document that action.

Caution: Exercise caution when acknowledging receipt of the claim by mail. The address on Form 14039 may be different from the address on ENMOD.

Note: Taxpayer notification does not apply to employees securing claims or documentation face to face from the taxpayer.

Note: An acknowledgement notice will generate systemically when paper returns are processed with SPC 8 or S.

- (6) After receipt of the taxpayer's claim/allegation, IRS will need to research the case to verify the taxpayer's claim is valid. Input TC 971 AC 522 UNWORK for each year affected, if none exists on the account, unless you are closing the case with an AC 501, AC 504 or AC 506 on the same day.

Note: TC 971 AC 522 will generate systemically when paper returns are processed with SPC 8 or S or when tax-related identity theft loose forms are scanned to CII.

Exception: If you have determined there was no identity theft (NOIDT), you must enter a TC 971 AC 522 UNWORK so it can be reversed with a TC 972 AC 522 NOIDT. The TC 972 AC 522 must be post-delayed one week to allow the TC 971 to post. No TC 972 AC 522 is necessary if you enter an AC 504.

See IRM 25.23.2.3.6, *When to Request Additional Information to Support an Allegation of Identity Theft*, for more information. If no acknowledgement letter has been sent, correspond to acknowledge receipt of the taxpayers claim, unless you are closing the case with an AC 501, AC 504 or AC 506 on the same day. Send the appropriate closing letter, instead.

25.23.2.3.1
(02-02-2024)

Dependent Identity Theft

- (1) Dependent identity theft can impact any individual.
- (2) Form 14039 or similar statement should be filed to report dependent identity theft. The dependent may self-report.

Reminder: Dependents can be any age, not just minors. We may receive a 14039 from a victim, their parent or guardian.

A parent or legal guardian of the dependent may submit a report of 'dependent identity theft' to IRS on behalf of the dependent. Form 14039 Section F must be completed in this situation. See IRM 25.23.2.2.1, *Taxpayer Interaction*, for information relating to all aspects of filing an identity theft claim.

- (3) The misuse of a dependent SSN, unrelated to tax administration, such as obtaining a credit card or driver's license in the dependent's name is considered non-tax related identity theft. See IRM 25.23.1.3, *Identity Theft and the IRS* for the definition of non-tax related identity theft and IRM 25.23.3.2.3, *Self-*

Identified - Non-Tax-Related Identity Theft - IDT4 Overview for processing Form 14039 for non-tax related identity theft.

- (4) The use of a dependent SSN on a tax return that lists them as a dependent is considered tax related identity theft if the person claiming the SSN does so without the dependent's knowledge or permission, unless the primary and/or secondary taxpayer on the return claiming them as a dependent is their parent or legal guardian. Individuals claimed as a dependent on a return filed by their parent or legal guardian are not victims of identity theft.

Caution: A transposed number, scrambled SSN, or mixed entity is not considered identity theft.

- (5) For claims of tax related identity theft, if the person claiming the dependent SSN on a return is the parent or legal guardian, a determination of "No IDT" will be made. The parent/legal guardian can file a paper return claiming the dependent if they meet the requirements to claim the dependent. They can also file a Form 15227, Application for an IP PIN, to protect the dependents TIN from identity theft.

Note: If the inquiring parent/legal guardian is not listed as the parent or the custodial parent listed on DDBKD, they will need to provide documentation of guardianship or custody when filing the Form 15227.

- (6) A TC 971 AC 501 will be required to mark the account for a taxpayer identified claim to generate a CP01A. This is necessary because victims of dependent identity theft may not be able to opt-in for an IP PIN with secure access digital identity (SADI). A TC 971 AC 506 with MISC code field of: WI ITVAA OTHER or WI ITVAC OTHER, will be required for an IRS identified dependent identity theft. Send the appropriate closing letter.
- (7) If the dependent who is determined to be a victim of identity theft is claimed on a fraudulent return that meets nullity return criteria, you will be required to resolve the fraudulent return account, if it has not already been resolved, in addition to processing the Form 14039. See IRM 25.23.4.8.2, *Streamline Identity Theft (IDT) Case Identification and Processing*. For dependent identity theft purposes, a return is considered valid if the income reported on the tax return is valid regardless of any dependent identity theft and any subsequent dependent related credits. .

Note: See IRM 25.23.4, *IDTVA Paper Process*, for more information. That IRM will provide specific instructions for research, procedures for marking the account and resolution of a claim. It will also provide guidance for situations of dependent IDT not addressed in this IRM.

25.23.2.3.2 (09-09-2021) Assessing the Scope of the Taxpayer's Issues

- (1) Taxpayers may initially come to IRS regarding a current year refund. Some taxpayers may not be aware that other tax modules have also been affected by identity theft.
- (2) Upon receipt/assignment of an identity theft case, an initial cursory review must be performed to identify all taxpayers and all taxpayer issues. Identifying issues at the beginning of the case provides a higher level of customer service and reduces the potential for problems to go unresolved.

Note: A taxpayer may file a claim of identity theft that covers multiple tax years. Each year **MUST** be evaluated based upon the facts and circumstances for that year.

- (3) Give special attention to cases that, by their nature, indicate a high potential for multiple year involvement. Although the following examples are not all inclusive, taxpayers who do not have a filing requirement are more susceptible to being targeted. This includes elderly, disabled and/or under-aged.

Example: A taxpayer's only income is Supplemental Security Income (SSI) paid by the Social Security Administration. A proposed reduction in SSI benefits due to an IRS levy has prompted the taxpayer to contact IRS and file a Form 14039, Identity Theft Affidavit, indicating his SSI was levied for a 2010 tax liability. Furthermore, the taxpayer states that they are permanently disabled and have not worked since 2007. Account review indicates returns filed for 2009, 2010, 2011, and 2012.

Example: A duplicate filing condition involves one return showing low wages, a filing status of single, and no dependents claimed. The other return shows a filing status of married filing joint (MFJ) with dependents claimed. Our records show that the taxpayer is 17 years old. While it is possible for a 17 year-old to file a MFJ return claiming dependents, the very nature of this case should cause the employee working the case to look at prior year accounts. In our example, the returns from prior years show the MFJ couple has been filing for a number of years under the SSN. Refer to your relevant operational IRM(s) for the appropriate action to be taken on the prior year's accounts.

Note: It is understood that multiple year involvement may not surface until a later phase in the processing of the case. Once multiple year involvement is determined, all issues **MUST** be addressed prior to case closure.

25.23.2.3.2.1
(09-06-2023)

Addressing All Taxpayer Issues

- (1) IRS is committed to providing taxpayers who have experienced identity theft with an additional level of sensitivity and understanding. From the taxpayer's perspective, his/her account encompasses all his/her tax returns.
- (2) Employees assigned an identity theft case will treat the identity theft victim's account as a whole, resolving all account issues.
- (3) Identity theft cases can be complex and involve multiple functions. Not all employees have the system access or delegated authority to take certain actions needed to completely resolve the taxpayer's issues.
- (4) In situations where you have multiple controls with another function, you must contact that functional employee or liaison. If there are multiple controls within IDTV groups, refer to IRM 25.23.4.3.2, *Case Transfer Within IDTV*, and Exhibit 25.23.4-7, *Identity Theft (IDT) Multiple Control Decision Document*, for additional information.
- (5) When identity theft issues involve multiple tax years or multiple taxpayers that may or may not be assigned or active (for example, "active" referring to a tax year with a balance due), every effort must still be made to ensure all issues are addressed and resolved. An IDRS control base must be opened for all tax

years impacted by identity theft. IDTVA functions, see IRM 25.23.4.3.1, *CII and IDRS Case Controls*, for more information.

- (6) To ensure taxpayers issues are not overlooked, the IDTVA has a multi-tier approach to determine where, and by whom, a case must be worked:
 1. **Internal IDTVA Transfer:** There may be situations when a case is transferred to another function within IDTVA for complete end to end resolution. Refer to IRM 25.23.4.3.2, *Case Transfer within IDTVA*.
 2. **External Transfer:** There may be situations when a case will be transferred to another function outside IDTVA for complete end to end resolution. For example: RICS, Field Operations, etc. Refer to Exhibit 25.23.4-5, *IDTVA Routing Matrix*.

25.23.2.3.3 (09-15-2020) Identity Theft Case Controls

- (1) All confirmed identity theft cases **MUST** be controlled. The case controls will remain in effect until all issues are resolved and the taxpayer is notified of actions taken. IDTVA employees will use the information provided in Exhibit 25.23.2-16, *IDTVA IDRS Category Controls by Function*, to control identity theft cases.

Note: Refer to specific IRM guidance to ensure you are following your function's established methods for controlling identity theft cases.

25.23.2.3.4 (09-06-2023) Required Case and History Notes

- (1) Throughout this IRM, and its chapters, there will be required case and history notes for Integrated Data Retrieval System (IDRS), Correspondence Imaging Inventory (CII), and/or Accounts Management Services (AMS) as it relates to the status of an identity theft case.
- (2) All actions taken on taxpayer accounts will be documented on CII, AMS and IDRS (CII actions systemically post a note on AMS). In addition, there may be functional specific systems that will require documentation of case actions and determinations.

Note: Cases worked through CII will automatically add a history item to AMS.

- (3) Case documentation will contain sufficient information to allow other employees to easily determine what actions were taken and what further actions are required to resolve the case. Accurate documentation promotes quality, prevents duplication of efforts by other employees, and enables phone assistants to provide accurate updates to phone inquiries.
- (4) Case documentation must include sufficient information to support the determination and describe actions taken to resolve the case. When applicable, include the following information:

Note: CII case notes can contain up to 500 characters. If more space is needed, create additional case notes.

- Case determination and information used to justify the determination. When documenting IRPTR, research may be necessary to provide specific payer document information.

Example: Based on IRPTR data TC 150 determined to be bad. TC 150 will be nullified.

Example: TRDBV and IRPTR researched. Case determined to be bad/good. Account will be adjusted to the taxpayer's TC 976 return.

- Document any forms sent to another area (e.g., Form 9409, Form 14394, Form 2859, etc.).

Note: See IRM 25.23.4.12.1, *Collection Activity – Form 14394*, and IRM 25.23.4.12.2, *Collection Activity – Form 13794 Additional Actions Required - Lien*. Also refer to IRM 25.23.13.3.1, *Form 9409 Procedures - IRS/SSA Wage Worksheet* for additional information.

- Document any case referrals to another function (e.g., cases referred to Exam, DITA, Appeals, etc.).
- Document the reason for not sending a closing letter.

- (5) If the AMS or CII system is down, then narratives and/or case notes will not be required when the case is worked. The narratives and/or case notes will be input when the system is available. Do not close the case until all actions have been completed.

25.23.2.3.5
(09-06-2023)
Identity Theft Research

- (1) Research must be performed and documented prior to reaching a final determination of identity theft. Research using Command Codes (CC) ENMOD, IMFOL, RTVUE, NAMES, INOLE, DUPOL, FFINQ, REINF, and IRPTR.

Caution: Consult your functional section of IRM 25.23, *Special Topics, Identity Protection and Victim Assistance*, for research requirements when resolving specific inventory types as the following list is not all inclusive.

Reminder: Inadequate authentication of the identity of a caller could result in an unauthorized disclosure of return or return information. Refer to:
IRM 11.3.2.4.1, *Individuals*
IRM 11.3.2.4.1.2, *Identity Theft and Access to Tax Returns and Information Returns*
IRM 21.1.3.2.3, *Required Taxpayer Authentication*
IRM 21.1.3.2.4, *Additional Taxpayer Authentication*
IRM 21.2.3.5.8, *Transcripts and Identity Theft*

- (2) Review all returns for the year(s) involved (including returns filed at other sites AND electronic filed returns).

- (3) Compare all claims and return information for:

- Name
- Social Security Number
- Address
- Occupation
- Exemptions
- Signatures (except for e-filed returns when a signature is unavailable)
- Similar tax data
- Forms W-2, etc.

- Marital status changes
- Tax return preparer
- Direct Deposit accounts

Note: See IRM 25.23.4.6.1, *Required Research* and IRM 25.23.4.6.2, *IDTVA - Additional Research and Required Actions*, for IDTVA research requirements.

- (4) Search returns, schedules, and forms for a different TIN. Research spouse and dependent information whenever available.

Note: Research Real-Time System (RTS) in addition to IDRS research of CCs for Individual Tax Identification Numbers (ITIN). See IRM 3.21.263.9.1.2, *Accessing and Logging onto ITIN Real-Time System (RTS)* and IRM 3.21.263.9.4, *Researching the ITIN RTS*.

- (5) Research the TIN (valid and invalid) to determine if there was a mixed entity or scrambled case in prior years, and to locate any possible cross-reference TIN.
 - a. A mixed entity is an inadvertent use of another taxpayer's TIN. This often occurs between family members. Research of Forms W-2 or previous returns can usually locate a different valid TIN for each taxpayer.
 - b. A true scrambled SSN case occurs when the Social Security Administration mistakenly assigns the same SSN to two different people. NUMIDENT will show different entries for name, date of birth, place of birth, and/or parents' names for the SSN owner.

Note: See IRM 21.6.2, *Adjusting TIN-Related Problems*, if your research indicates that the case may be a mixed entity or a scrambled SSN instead of identity theft.

- (6) Search entity modules for indications of identity theft such as identity theft claims attached to the return or a previously posted TC 971 with Action Code (AC) 5XX.
- (7) Utilize IAT Tools- refer to functional IRMs for mandatory IAT tools and to Exhibit 21.2.2-2, *Accounts Management Mandated IAT Tools*, for additional information.

25.23.2.3.5.1 (09-15-2020) **Economic Impact Payments – General Information**

- (1) The Coronavirus Aid, Relief, and Economic Security Act (CARES Act), which was signed into law on March 27, 2020, added new section IRC 6428 to the code. Section 6428 directed the IRS to issue advance payments of the recovery rebate credit, also referred to as Economic Impact Payment (EIPs or EIP 1) to eligible individuals. A second Economic Impact Payment (EIP 2) was authorized by the Consolidated Appropriations Act of 2021 and a third Economic Impact Payment (EIP 3) was authorized by the American Rescue Plan Act of 2021.
- (2) For more information on eligibility and other requirements for the EIP, see IRM 21.6.3.4.2.13, *Economic Impact Payments (EIP)*, and IRM 25.23.4.20, *Economic Impact Payment (EIP) and Recovery Rebate Credit (RRC) - General*.
- (3) If you receive a call requesting account information regarding the EIP, perform high-risk disclosure and research the account. For more information, see IRM

21.6.3.4.2.13.1, *Economic Impact Payments - Account Information*, IRM 25.23.4.20.1, *Economic Impact Payment (EIP) Account Research* and IRM 25.23.4.20.2, *Economic Impact Payment (EIP) – Additional Research for Identity Theft (IDT) Cases*.

25.23.2.3.6
(09-15-2020)

**When to Request
Additional Information to
Support an Allegation of
Identity Theft**

- (1) Whether a case begins because IRS has identified a tax-related identity theft or because a taxpayer has identified himself or herself as an identity theft victim, additional information may be required. If we can't resolve the account using internal information and/or information already provided by the taxpayer, request additional information. Taxpayer information to substantiate identity theft may include:

- a. Authentication of Identity - a copy of a current, valid form of identification (examples include a driver's license, state identification card, social security card, or passport).

Reminder: Any current US federal or state government issued identification presented **MUST** be signed by the taxpayer (or Legal Guardian if a minor).

Exception: Minor's Social Security cards should NOT be signed.

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

- b. Evidence of Identity Theft - Form 14039, Identity Theft Affidavit.

Note: Only request a Form 14039 when the taxpayer has not previously submitted the form or when the submitted form is illegible.

- c. Payor documents, such as Forms W-2 or 1099,
d. and utility bills, deeds or other proof of residency.

- (2) Advise the taxpayer to enlarge photocopies, if necessary, so all information and pictures are clearly visible. If taxpayers do not provide additional information when requested, proceed with case resolution assuming the taxpayer is not an identity theft victim.
- (3) The business unit/function that is assigned the identity theft case or issued the notice/letter relating to the identity theft must follow their functional procedures for soliciting additional information.
- (4) Before requesting additional information, review the taxpayer's account (ENMOD/IMFOLE) to determine if a TC 971 (AC 501, 504, 505, 506, or 522) identity theft indicator exists and the related tax years. Previously submitted taxpayer information or case information may allow you to make an internal determination without further taxpayer contact. For example:
1. TC 971 AC 501 - Taxpayer initiated tax-related identity theft incident
 2. TC 971 AC 504 - Miscellaneous codes indicating taxpayer initiated non-tax-related identity theft incident: ACCT, ACCT-M, BOTH, BOTH-M, EMPL, EMPL-M, NKI or NKI-M

3. TC 971 AC 505 -PGLD inputs TC 971 AC 505 on an account even when an identity theft indicator code (AC 501, 504, or 506) is present on the account.

Note: For more information about this indicator, refer to IRM 25.23.2.8.2, *IRS Data Breaches - TC 971 AC 505*.

4. TC 971 AC 506 - IRS identified tax-related identity theft incident
5. TC 971 AC 522 - with any of the following Administration Source Codes present: INCOME, MULTFL, INCMUL, NOFR, OTHER, NODCRQ, IRSID or UNWORK

Note: This excludes accounts marked with a TC 971 AC 522 reflecting "PPDS" as the BOD, "OPIP" as the Program, and "OTHER" as the Tax Administration Code

- (5) Review AMS history to assist in determining if the scanned documents were initially presented in person. For taxpayers who present their documents in the TAC, determine if the Form 14039 or police report is annotated in the upper right corner with an "S". See paragraph 2 of IRM 21.3.4.28.1, *Tax Return Related Identity Theft Issues*. If the "S" is present, then the TAC employee reviewed and verified the documents presented and that they were valid. If the "S" is not present, then the TAC employee was unable to verify the taxpayer is the correct taxpayer.

Reminder: If sufficient internal information is present, do NOT request the taxpayer submit or resubmit a claim. However, if sufficient information is not available and/or more than 45 days has passed since the taxpayer mailed their information, request the taxpayer to resubmit their claim/ information and annotate AMS.

Note: If a TC 971 AC 522 WI SP PNDCLM is present, request the original return. Additional identity theft information will be attached to the return.

- (6) Additional information can be accepted from the taxpayer, third party or someone who has power of attorney for the taxpayer (e.g., Form 2848, Power of Attorney and Declaration of Representative).

25.23.2.3.7 (12-06-2022) When to Update the Victim's Address

- (1) When a return posts to an account as a TC 150, the address is updated systemically to the address on that return. Consequently, when a return filed by a non-TIN owner posts to an account as a TC 150, the address on ENMOD is updated to the address on that return. Therefore, it is important to make timely entity corrections to prevent the issuance of correspondence or refunds to the wrong address. Check IDRS for pending address changes.
- (2) Taxpayers may request a change of address using a Form 8822, IMF Change of Address Request, by correspondence, or by phone through oral statement. Refer to IRM 3.13.5.52, *Form 8822, IMF Change of Address Request*, and IRM 21.1.3.20, *Oral Statement Authority*, for additional information.
- (3) After confirming the person you are working with is the SSN owner, per IRM 25.23.2.3.5, *Identity Theft Research*, you will need to verify that the address posted on ENMOD/IMFOLE/BMFOLE is the correct address. Correct the address when appropriate. Refer to IRM 21.2.4.3.5, *Address Change/*

25.23 Identity Protection and Victim Assistance

Correction. Correcting the address as early as possible may prevent disclosure of taxpayer information.

Exception: Updating the address on controlled identity theft cases does not apply to telephone assistants or Field Assistance employees. Addresses are updated by the assigned employees only after research is completed, an SSN owner determination made and the case resolved. Refer to IRM 25.23.12.4.1, *Telephone Inquiries Regarding Identity Theft Victim Assistance (IDTVA) Tax-Related Cases*, and IRM 21.1.3.20, *Oral Statement Authority*, for additional information.

Exception: Oral Statement Authority does not apply if the current address is a Service Center Address. Advise callers to submit requests for address changes using Form 8822 or by correspondence (as long as the request contains the same information as the Form 8822). See (6) and (7) below for guidance.

Caution: Use a posting delay code as needed when updating the address and inputting account adjustments at the same time. The address change must post first, unless it would prematurely release an S- freeze and cause an erroneous refund

Note: The submission of Form 14039, Identity Theft Affidavit, by a claimant is not proof of identity theft and address changes should not be based solely on receipt of this form. Form 14039, Identity Theft Affidavit, must be used in conjunction with other key information to make decisions related to verifying taxpayer information. Refer to IRM 25.23.2.3.5 , *Identity Theft Research*, for additional information.

- (4) Change the address on MF to the new address (line 7) of Form 8822, Change of Address, if the taxpayer provides proof of identity document or other key information.
- (5) The taxpayer can request a change of address in writing as long as the request contains the same information as the Form 8822, Change of Address:
 - The new address
 - The taxpayer's full name
 - The taxpayer's signature, or the signature of an authorized representative
 - The old address
 - Social security number, employer identification number, or individual taxpayer identification number

Per Rev. Proc. 2010-16, a valid request for a change of address must be a clear and concise request for the purpose of changing the address. Filers of a joint return must provide both names, social security numbers, and signatures. Individuals who have changed their last name with SSA must provide the last name shown on the most recently filed return and the new last name. Verify the old address through research and input the change of address via CC ENMOD/ENREQ.

- (6) If the current address shown on CC ENMOD/IMFOLE is a Service Center/ Campus Address, research for a prior address (prior tax return data, IRP

documentation, CII documentation or history) to verify the prior address from the taxpayer's Form 8822, correspondence, etc.

- a. If prior address research shows an address that matches, change the taxpayer's address.
 - b. If prior address research shows an address (other than on a fraudulent return) that does not match the prior address on taxpayer's Form 8822 or correspondence, contact the taxpayer using 104C letter or other appropriate letter for a correct address.
- (7) If there is no prior tax return data for the taxpayer and/or no IRP documentation, or if IRP document shows an "in care of" name and different address, and CII does not show any document or history to verify the prior address, and taxpayer sent a signed, government issued ID, check for a current address on the ID document.
- a. If the taxpayer's signed, government issued ID has an address that matches the current address entered on the taxpayer's Form 8822 or in the taxpayer's correspondence, change the taxpayer's address.
 - b. If the signed, government issued ID does not have an address or has a different address than given on the Form 8822 or in the correspondence, contact the taxpayer for a correct prior/current address either by telephone or using the Letter 104C or other appropriate letter
- (8) Attempt telephone contact with the taxpayer or representative whenever possible. During telephone contact, verify the taxpayer's phone number on IDRS for all account related calls in which disclosure verification has occurred. Add or update phone numbers on IDRS and specify the type of number, (i.e., home, cell, etc). If contact information is provided on correspondence and it is determined to be from the valid TIN owner, add or update the phone number(s) on IDRS. Do not close the case until all actions have been completed.

25.23.2.3.8
(05-08-2023)

Marking Taxpayer Accounts When Accepting Identity Theft Claims

- (1) Upon receipt of a claim, mark the taxpayer's account using Command Code (CC) REQ77 initiated from ENMOD to input a TC 971 AC 522 UNWORK.

Reminder: If, at the time of case closure you find the Entity module has not been flagged with a TC 971 AC 522 PNDCLM, UNWORK or IRSID, do not input this code at closing. Close the identity theft issue with TC 971 AC 501 or AC 506, as appropriate

Reminder: Identity Theft indicators AC 501, AC 504, AC 505, AC 506, AC 522, AC 523, AC 524 and AC 525 never expire. In addition, once a taxpayer is in the IP PIN population, they cannot be removed.

- (2) The Secondary Date field on CC REQ77 is limited to the current calendar year (cannot be the current day or any future date) and 7 prior years. The secondary date field will not allow the input of any date outside that range. If the year in question is earlier than the oldest allowable year, See IRM 25.23.2.3.8.1, *Command Code REQ77 Secondary Date and Old Case Year Issue* for more information.

Note: If the allegation or suspicion of IDT is for an Economic Impact Payment (EIP), check the TC 971 AC 199 on IMFOLE to see the source of the EIP. If the source is a 2018 return, input 2018 as the tax year affected by IDT. If the source is something other than a 2018 return, input 2019 as the tax year affected.

- (3) After receipt of the taxpayer's claim, the employee assigned will need to research the case to verify the taxpayer's claim and determine the appropriate action(s) needed. If it is later determined that identity theft did not occur, reverse the TC 971 AC 522 (refer to Exhibit 25.23.2-11, *TC 972 AC 522 - Reversal of the TC 971 AC 522*). Follow your IRM procedures to notify the taxpayer of your determination.
- (4) A systemic notification letter is sent once a valid case is resolved and the TC 971 AC 501 is input.

Reminder: The CP01 is only issued once in a 3-year period. If a TC 971 AC 501 posted on the account within the last three years, a closing letter is required.

25.23.2.3.8.1
(06-17-2024)

**Command Code REQ77
Secondary Date and Old
Case Year Issue**

- (1) CC REQ77 with Transaction Codes 971 or 972 is used to input, update and reverse the identity theft Action Codes that mark and close identity theft cases.
- (2) The Secondary Date field on CC REQ77 is limited to the current calendar year (cannot be the current day or any future date) and 7 prior years. The secondary date field will not allow the input of any date outside that range. If the year in question is earlier than the oldest allowable year, input the TC 971 or TC 972 and the appropriate AC 5XX on the oldest allowable year and leave an AMS and ENMOD history indicating which year was affected by identity theft.

Exception: IDTVA Employees ONLY - Refer to box 11 of the table in Exhibit 25.23.4-21(8), *Input, Annotations and Action Requirements for Streamline/Non-Streamline Case Processing*, for separate instructions on reversals of existing IDT indicators with a secondary date older than 7 years old.

- (3) On ENMOD, each tax year must have a history item. See the table below for specific scenarios.

Transaction Code and Action Code	AMS History	CC ENMOD History
TC 971 AC 501	"Closed XXXX tax year with AC 501" (add any necessary details)	AC501XXXX
TC 971 AC 504	"Closed XXXX tax year with AC 504" (add any necessary details)	AC504XXXX

Transaction Code and Action Code	AMS History	CC ENMOD History
TC 971 AC 506	"Closed XXXX tax year with AC 506" (add any necessary details)	AC506XXXX
TC 971 AC 522	For UNWORK : "Received valid claim for XXXX tax year" (add any necessary details) For IRSID : "Discovered IDT on XXXX tax year." Notate how it was discovered. For PNDCLM : "TP alleges IDT for XXXX"	AC522XXXX
TC 972 AC 501	"No IDT on TY XXXX"	NOIDTXXXX
TC 972 AC 504	"No IDT on TY XXXX"	NOIDTXXXX
TC 972 AC 506	"No IDT on TY XXXX"	NOIDTXXXX
TC 972 AC 522	"No IDT on TY XXXX"	NOIDTXXXX

25.23.2.3.9 (10-01-2022) Taxpayer Advocate Service

- (1) The Taxpayer Advocate Service (TAS) is an independent organization within the Internal Revenue Service (IRS), led by the National Taxpayer Advocate. Its job is to protect taxpayers' rights by striving to ensure that every taxpayer is treated fairly and knows and understands their rights under the Taxpayer Bill of Rights (TBOR). TAS offers free help to taxpayers, including when taxpayers face financial difficulties due to an IRS problem, when they are unable to resolve tax problems, they haven't been able to resolve on their own, or when they need assistance to address an IRS system, process, or procedure that is not functioning as it should. TAS has at least one taxpayer advocate office located in every state, the District of Columbia, and Puerto Rico.
- (2) Refer taxpayers to TAS when the contact meets TAS criteria and you can't resolve the taxpayer's issue the same day Refer to IRM 13.1.7.3, *TAS Case Criteria*. The definition of "same day" is within 24 hours. "Same day" cases include cases you can completely resolve in 24 hours, as well as cases in which you have taken steps within 24 hours to begin resolving the taxpayer's issue. See IRM 13.1.7.5, *Same Day Resolution by Operations*. In cases where the taxpayer states he has a hardship, use sufficient probing to determine that a manual refund is required before referring to TAS. For additional information refer to IRM 21.1.3.18, *Taxpayer Advocate Service (TAS) Guidelines*.

25.23.2.3.10
(10-01-2024)
**Electronic Products
Service and Support
(EPSS) Disabled
Accounts**

- (3) Taxpayers may request assistance during or after enforcement action. The request must meet criteria as listed in IRM 13.1.7.3, *TAS Case Criteria*. The identifying function will prepare Form 911, Request for Taxpayer Advocate Service Assistance (And Application for Taxpayer Assistance Order).

- (1) Compromised on-line accounts are disabled, preventing SSN owners from accessing the account. EPSS employees will flag the account with a TC 971 AC 522 EPSS DISABL.

Caution: Prior to January 2015, the acronym NODCRQ was used when the taxpayer reports a second incident of identity theft and taxpayer information was previously provided.

- (2) Taxpayers are instructed by EPSS to file Form 14039 to secure an IP PIN to protect their compromised SSNs.

1. If the Form 14039 is received, due to a disabled account, input a TC 971 AC 522 UNWORK, if none already exists.
2. Input TC 971 AC 506 WI AM OTHER to move the taxpayer into the CP01A population.

If not tax-related issue: Issue a 4402C letter with paragraph A, F, I and L (insert the language below in paragraph F): "To further protect you, we will issue you an IP PIN by mail starting in Mid-December and it should be received by Mid-January. You will need an Identity Protection PIN to file your tax returns in the future."

Caution: If the TC 971 AC 506 is not input prior to cycle 47 of the processing year (meaning an IP PIN/CP01A will **not** generate for the upcoming filing season) do **not** include paragraph F because no IP PIN will be issued for the upcoming year.

If tax-related issue: Notify the taxpayer (victim), via Letter 4674C, to inform the taxpayer the actions you took.

Caution: Do **NOT** include any paragraphs that refer to obtaining an IP PIN online, as these accounts are blocked.

. This victim notification letter will include: 1. Information about identity theft prevention. 2. Information about identity theft related resources. 3. Information about the identity theft indicator placed on his or her account. 4. Provide information about the IP PIN.

25.23.2.4
(09-15-2020)
**IDT Indicators – Tax
Related**

- (1) Identity Theft Action Codes (AC) are used to Identify types of identity theft cases. In the following subsections we will define the Tax-Related ACs. For other Miscellaneous identity theft ACs, see IRM 25.23.2.8, *Miscellaneous Identity Theft Indicators*.

25.23.2.4.1
(02-02-2023)
**Tracking and Reporting
Identity Theft Cases -
Identity Theft Indicators**

- (1) IPSO developed identity theft indicators as a method to track identity theft cases from the time a taxpayer or the IRS initially suspects identity theft through case closure. Identity Theft Action Codes (AC) are used with TC 971 to mark the entity modules of accounts on which identity theft is a factor. Identity theft can be tax-related or non-tax-related. Identity theft cases can be found in virtually any BOD/Function inventory. The identity theft indicators are as follows:

(2)

Action Code	Description	Used by	IRM Guidance located in:	IP PIN/Delivery Method
501	Identity Theft Case Closure (tax-related) - Taxpayer Initiated.	All functions	IRM 25.23.2.6.1, <i>Closing Taxpayer Initiated Identity Theft Affecting Tax Administration - TC 971 AC 501.</i>	Yes/CP01A
504	Identity Theft Case Closure (Non-tax-related) - Taxpayer Initiated. - TC 971 AC 504 with Miscellaneous Field Codes ACCT, ACCT-M, BOTH, BOTH-M, EMPL, EMPL-M, NKI or NKI-M are reserved for use by IDTVA-I employees. Tax-related identity Theft - TC 971 AC 504 - Miscellaneous Field Code SPCL1, SPCL2, RPM1, RPM2, RPM3, RPM4, and EAFail	Non-tax-related identity theft - IDTVA-I ONLY for additional information. Tax-related identity Theft - as designated.	Non-tax-related identity theft: IRM 25.23.2.8.1.1, <i>TC 971 AC 504 with Miscellaneous Field Codes ACCT, ACCT-M, BOTH, BOTH-M, EMPL, EMPL-M, NKI or NKI-M</i> Tax-related identity Theft: IRM 25.23.2.8.1.2, <i>TC 971 AC 504 - Miscellaneous Field Code SPCL1, SPCL2, RPM1, RPM2, RPM3, RPM4, and EAFail</i>	TC 971 AC 504 with Miscellaneous Field Codes other than SPCL1, and EAFail are eligible to Opt-in to the IP PIN program.

Action Code	Description	Used by	IRM Guidance located in:	IP PIN/Delivery Method
505	IRS loss of PII -IRS identified, taxpayer not required to provide required ID theft claim	PGLD Only	IRM 25.23.2.8.2, <i>IRS Data Breaches</i> - TC 971 AC 505	Opt-in. Exception: If the taxpayer's on-line account is blocked, because of the nature of the breach, they need to file a Form 14039 for an IP PIN and could have IP PIN issued via CP01A.
506	IRS determined identity theft - Taxpayer is not required to provide ID theft claim, unless requested.	All Functions	IRM 25.23.2.6.3, <i>Closing IRS Determined Identity Theft Affecting Tax Administration</i> - TC 971 AC 506.	Automatically entered in the IP PIN program.

#

Action Code	Description	Used by	IRM Guidance located in:	IP PIN/Delivery Method
522	Provides the status of an identity theft issue: <ul style="list-style-type: none"> Taxpayer initial allegation IRS initial suspicion Receipt of valid taxpayer claim and (if requested) additional information. 	All functions	IRM 25.23.2.4.4.1, <i>IMF Identity Theft-Taxpayer Initiated Allegations of Identity Theft - TC 971 AC 522</i> , IRM 25.23.2.4.5, <i>IRS Initiated Suspicion of Identity Theft - TC 971 AC 522 IRSID and IRM 25.23.2.3, Identity Theft Claims - General Guidelines.</i>	No
			Reserved	No
524	Locking Decedent Accounts	IPSO and Return Integrity and Compliance Services (RICS) TPP.	IRM 25.23.2.8.4, <i>Locking Decedent Accounts - TC 971 AC 524.</i>	No
525	Employment-related Identity Theft	Systemic Input ONLY	IRM 25.23.2.8.5, <i>Employment-related Identity Theft – TC 971 AC 525.</i>	Opt-in

#

(3) The Service utilizes a variety of methods to ensure all identity theft related inventory is tracked within specific inventories.

(4) The indicators used on identity theft cases provide the Service with data reflecting the case status (the list below is not all-inclusive). The specific indicators are discussed at length later in this IRM.

- New taxpayer claims of identity theft
- Newly identified suspicions of identity theft (no final determination of identity theft)
- Resolved identity theft case

25.23.2.4.2 (10-01-2018) Tracking IMF Tax-Related Identity Theft Inventory

(1) In situations where the taxpayer makes an allegation of identity theft or when the IRS initially suspects that identity theft may have occurred, IRS functions will apply an identity theft indicator. The identity theft tracking indicator alerts others that a claim of identity theft has been reported. Refer to IRM 25.23.2.4.4, *Initial Allegation or Suspicion of Identity Theft - Identity Theft Indicators*, for additional information regarding the appropriate tracking indicator.

Note: The application of the TC 971 AC 522 PNDCLM or UNWORK does not always equate to an inventory point of count. Refer to your functional IRM regarding the process of inventory management for Identity Theft cases.

- (2) In most instances, for taxpayer initiated claims of identity theft, the case **MUST** be moved into identity theft inventory once the taxpayer has submitted a claim of identity theft and (if requested) provided additional information. This provides victims with a treatment stream for case resolution specific to identity theft. For additional information regarding identity theft documentation, refer to IRM 25.23.2.3, *Identity Theft Claims - General Guidelines*.
- (3) If after the account has been marked with an IMF Identity Theft Indicator, the employee determines identity theft did not occur, the IMF ID theft tracking indicator will be reversed by the employee assigned. This removes the case from identity theft inventory. See Exhibit 25.23.2-11, *IMF Only TC 972 AC 522 - Reversal of TC 971 AC 522*, for additional information. All other non-identity theft issues will be resolved using normal procedures.

25.23.2.4.3

(12-06-2022)

Tracking Individual Taxpayers Reporting to be Victims of Business-Related Identity Theft

- (1) Identity thieves sometimes use the PII of individuals to establish fictitious businesses. Many times, the fictitious business is used to support the filing of fraudulent IMF returns.
- (2) Employees will verify the IMF taxpayer's association with the EIN and determine if potential BMF ID theft exists prior to marking the IMF account with a tracking marker.

Example: Jane Smith calls an IMF related toll-free line to report she believes she is a victim of business-related identity theft and she is concerned her personal identity has been stolen. She received an IRS notice demanding payment for unpaid employment taxes on Jane's Flowers located in Florida (Jane is located in Maine). Jane has never owned a business and never resided in Florida. Jane provides the CSR with her SSN and the EIN on the notice.

- (3) Research to determine if there is a potential BMF ID theft issue **MUST** be completed prior to marking an account and referring or transferring the case/call to another area. Researching the account will allow the employee to determine if the case should be referred to the BMF ID theft inventory or moved/transferred into the regular BMF inventory following normal procedures.
 - Research CC BMFOLE (the business entity module) to determine if the taxpayer's SSN is associated with the EIN. BMFOLE contains a XREF SSN FIELD that will provide the associated SSN. The format for CC BMFOLE is BMFOLEXX-XXXXXXX
 - Research BMFOLI to look at filing and payment history. Returns filed with no payments **may** indicate fraudulent filings.
 - Research CC IRPTRI to review all Forms W-2 filed under a given EIN. Reviewing the individual accounts associated with the W-2s may assist in determining if the case needs to be moved into the BMF ID theft inventory. IMF accounts with ID theft indicators or RIVO involvement may support the BMF ID theft claim. CC format is IRPTRIX-XXXXXXXX4YYYY21 (4=valid EIN, 21=Forms W-2)
 - Research the IMF account to see if the EIN has been used on any IMF filings (i.e., Schedules C or H). If it is determined the EIN has been used for purposes other than intended, this may support the BMF ID theft claim.
- (4) Once the research is completed and it is determined there is potential ID theft, research CC IMFOLE to determine if there is an existing TC 971 AC 504

SPCL2. If there is currently no ID TC 971 AC 504 SPCL2 marker, the SSN entity must be marked using CC REQ77 with a TC 971 AC 504 SPCL2 as indicated in IRM 25.23.2.8, *Miscellaneous Identity Theft Indicators*. Include the EIN, if available, in the XREF TIN field on CC REQ77.

Reminder: The AC 504 will NOT accept an SSN in the XREF TIN field.

This will record ID theft of the individual's information for fraudulent BMF usage. Refer to Exhibit 25.23.2-4, *IMF Only TC 971 AC 504*, for additional information.

- (5) If the inquiry is received by phone, obtain all of the facts of the case including the EIN, business name and any other important information. For example:

- What notice the taxpayer received.
- If there is a current or former relationship to the business.
- What has been affected by the BMF ID theft (lien, levy, etc.).

Document all this information on the Form 14566, BMF Identity Theft Referral. Refer to IRM 25.23.9-6, *Business Master File (BMF) Identity Theft Referral Form*, for guidance on completion of Form 14566. Do not advise the taxpayer to submit a Form 14039 or Form 14039-B, Business Identity Theft Affidavit. Send the completed Form 14566 by secure email to your functional liaison. See <http://serp.enterprise.irs.gov/content/irm-supplements/identity-theft-bmf.html>. In the explanation on Form 14566, include any actions that you have input or will be inputting on the SSN. Do not hold cases for completion. Continue appropriate IMF account actions when a referral has been sent to BMF IDT. Link CII cases to expedite processing. Advise the caller that the case needs to be referred to the business identity theft function.

- (6) Include information on the Form 14566 that could help the functional liaison route the case to the appropriate area, such as:

- CAWR assessment- TC 290 assessment in blocking series 55- CC TXMOD
- Exam assessment- TC 300 assessment- CC TXMOD
- 6020b assessment - TXMOD RCC "4" and literal "6020b" at the end of the TC 150 assessment-CC TXMOD
- SFR assessment- SFR literal at the end to the TC 150 assessment - CC TXMOD
- Field Exam- Cases have a Primary Business Code 201 through 215, 301 through 309, and 315- CC AMDISA
- Field Collection- SC status 26
- ACS- SC status 22
- AM (BMF)- Any case that does not meet other account criteria

Reminder: You will always send referrals to your functional liaison. Your functional liaison will forward the referral to the appropriate area. Functional liaison guidance can be found at IRM 25.23.9.3, *Business Master File (BMF) Identity Theft Liaisons*.

- (7) Document AMS/CII, if available, to reflect the referral sent, the suspicious EIN and how the taxpayer became aware of the problem.

Example: Referral emailed to BMF ID theft CAWR Liaison. TP received notice of CAWR assessment. TP states they were not involved with EIN XX-XXXXXXX. (Include any other information employee deems important)

Caution: If the case needs to be reassigned on AMS/CII and an EIN is not available, reassign using all zeros for the EIN. Do not put the taxpayer’s SSN in EIN format.

(8) If the taxpayer filed a Form 14039 or other written documentation to advise the IRS of ID theft relating to a business/BMF issue, a referral must be sent to the BMF functional liaison. Attach the Form 14039 and Form 14039B, if available, to the secured email when referring the case to the liaison. The BMF IDT employee will send the appropriate acknowledgment letter. IMF employees must follow the same procedures for phone inquiries above to research the account, prepare a referral to a BMF IDT liaison, input a TC 971 AC 504 SPCL2, and update AMS/CII. Allow 30 days for a response from BMF IDT.

25.23.2.4.4
(10-01-2024)
Initial Allegation or
Suspicion of Tax-Related
Identity Theft - IMF
Identity Theft Indicators

- (1) An initial allegation or suspicion of identity theft can be recognized by either the taxpayer or the IRS. IPSO developed tracking indicators to mark taxpayer accounts when the identity theft incident is initially alleged or suspected.
- (2) Three Tax Administration Source codes were developed to track cases as they are initially identified:
- **TC 971 AC 522 PNDCLM** - for taxpayer initiated allegations of identity theft.
 - **TC 971 AC 522 UNWORK** - for submitted identity theft claims via Form 14039, police report or other accepted correspondence.
 - **TC 971 AC 522 IRSID** - for IRS initiated suspicions of identity theft.

#

- (3) Prior to marking an account with TC 971 AC 522 PNDCLM, UNWORK or IRSID, research ENMOD/IMFOLE to ensure the questionable tax year has not already been marked. **If the coding already exists, do not input a second, matching code for the same tax year.**
- (4) When the identity theft victim is the secondary TIN on a joint account, the identity theft indicator is input on the secondary SSN. Identity theft indicators are not input on the primary TIN in these instances. If both primary and secondary taxpayers are victims, place the appropriate indicator on both TINs.

Note: If an identity theft allegation/Form 14039 is submitted by one spouse on behalf of the other, or the allegation indicates that both spouses are victims but only one Form 14039 was filed, the case will be treated as an instance of “taxpayer initiated claim of identity theft.” However, if the claim is filed under one TIN, with no mention of a spouse, and during research an employee determines the IDT victim is the spouse, the case will be treated as an instance of “IRS determined identity theft” for the IDT victim.

- (5) Taxpayer entity modules can accommodate a limited number of transactions. Due to the entity limitations, we must also limit the number of TC 971 AC 522s applied to the account.
- (6) The secondary date on command code REQ77 will reflect the tax year of the incident. Apply a TC 971 AC 522 only once per tax year affected by identity theft. If there is an existing TC 971 AC 522 PNDCLM, UNWORK or IRSID for the same tax year, do not apply a second, matching code to that tax year. If there is an existing TC 971 AC 522 PNDCLM, UNWORK or IRSID refer to the table below:

Note: If the allegation or suspicion of IDT is for an Economic Impact Payment (EIP), check the TC 971 AC 199 on IMFOLE to see the source of the EIP and use the appropriate tax year. For an example if the source is a 2018 return, input 2018 as the tax year affected by IDT.

Note: A PNDCLM code means the taxpayer alleged identity theft. The code UNWORK means a claim has been received.

IF	THEN
<p>Your BOD or Function differs from that of the existing TC 971 AC 522 PNDCLM, NODCRQ, or IRSID for the same tax year</p> <p>Example: There is an existing TC 971 AC 522 PNDCLM input by WI FA for 2012. You are located in SBSE Compliance and have a TY 2012 issue.</p> <p>Reminder: Beginning in 2015, NODCRQ is used in conjunction with BOD PPDS and Program OPIP (TC 971 AC 522 PPDS OPIP NODCRQ) to identify/track on-line accounts disabled due to identity theft. Prior to 2015, NODCRQ was applied when the taxpayer claimed identity theft and there was a posted TC 971 AC 501/ 506.</p>	<p>Apply TC 971 AC 522 UNWORK to indicate a claim has been received.</p> <p>For additional information regarding multiple tax years, refer to IRM 25.23.2.4.4.1, <i>IMF Identity Theft- Taxpayer Initiated Allegations of Identity Theft - TC 971 AC 522</i>.</p>

IF	THEN
<p>You would have selected a different Tax Administration Code than was selected by the initial function receiving the additional information.</p> <p>Example: There is a TC 971 AC 522 IRSID for TY 2013 and you would have input an UNWORK</p>	<p>Apply TC 971 AC 522 UNWORK to indicate a claim has been received.</p> <p>For additional information regarding multiple tax years, refer to IRM 25.23.2.4.4.1, <i>IMF Identity Theft- Taxpayer Initiated Allegations of Identity Theft - TC 971 AC 522</i></p>
<p>There is an existing unreversed TC 971 AC 522 PNDCLM or IRSID and you determine the identity theft affected an additional tax year.</p> <p>Example: There is a TC 971 AC 522 PNDCLM for TY 2012 and you determine that TY 2011 was also affected by ID theft.</p>	<p>Apply TC 971 AC 522 UNWORK to the additional year(s) affected.</p> <p>In this example, apply a TC 971 AC 522 UNWORK to both TY 2011 and TY 2012.</p>
<p>There is an existing TC 971 AC 522 PNDCLM for a tax year not affected by identity theft.</p> <p>Example: The taxpayer claims identity theft for TY 2013 and there is an existing TC 971 AC 522 PNDCLM for 2012 and you have determined TY 2012 was NOT affected by identity theft.</p>	<p>For additional information refer to IRM 25.23.2.6.6.2, No Identity Theft (NOIDT) Determinations – TC 972 AC 522 NOIDT.</p> <p>In this example, you will reverse the TC 971 AC 522 PNDCLM for tax year 2012.</p>

Caution: Duplicate AC 522's will unpost and auto-delete.

- (7) The Secondary Date field on CC REQ77 is limited to the current calendar year (cannot be the current day or any future date) and 7 prior years. The secondary date field will not allow the input of any date outside that range. See IRM 25.23.2.3.8.1, *Command Code REQ77 Secondary Date and Old Case Year Issue* for more information.
- (8) Do not apply the AC 522 PNDCLM, UNWORK or IRSID to the SSN of a taxpayer when an **ITIN taxpayer reports** the misuse of the SSN. See IRM 25.23.2.6.1, *Closing Taxpayer Initiated Identity Theft Affecting Tax Administration - TC 971 AC 501*.

Example: In the course of performing an audit, the employee identifies an ITIN taxpayer has been working under the SSN belonging to another individual. The SSN owner is unaware of the misuse of his SSN. Do not apply the AC 522 to the commonly used SSN.

- (9) All identity theft affected accounts will require resolution and the application of a closing identity theft marker (TC 971 AC 501 or TC 971 AC 506), as applicable.

25.23.2.4.4.1
(02-02-2023)
**IMF Identity Theft-
Taxpayer Initiated
Allegations of Identity
Theft - TC 971 AC 522**

- (1) In situations where the taxpayer or the taxpayer's authorized representative as defined in IRM 21.3.7.5, *Form 2848, Power of Attorney and Declaration of Representative and Form 8821, Taxpayer Information Authorization Overview*, makes an allegation of identity theft, employees will mark the entity account, using Command Code (CC) REQ77 initiated from ENMOD to input a TC 971 AC 522 reflecting a Tax Administration Source Code PNDCLM, if none already exists. See Exhibit 25.23.2-10, *IMF Only TC 971 AC 522 Tax-Related Identity Theft Case Status (Initial Claim/Suspicion)*, for additional information.

Note: If the allegation or suspicion of IDT is for an Economic Impact Payment (EIP), check the TC 971 AC 199 on IMFOLE to see the source of the EIP. Use the tax year the EIP was based on as the tax year affected by IDT. See IRM 21.6.3-2, *TC 971 AC 199 MISC Field Descriptions for Economic Impact Payments (EIPs)*.

Reminder: If the taxpayer is alleging identity theft on more than one tax year, input AC 522 PNDCLM for each tax year, but only if a TC 971 AC 522 PNDCLM does not already exist for the specific year. Prior to marking an account with a TC 971 AC 522 PNDCLM, UNWORK or IRSID, research ENMOD/IMFOLE to determine if the questionable tax year has been marked this will ensure you are not inputting duplicate transactions. There will be only one PNDCLM, UNWORK or IRSID per tax year.

Example: Taxpayer calls the IRS on March 13, 2017, regarding a CP 2000 notice for 2015. He states he did not earn the income reported nor did he reside in the state in which the income was earned. He suspects he may be a victim of identity theft. He has not experienced a previous identity theft issue. He is concerned that someone may be using his SSN without his permission for employment purposes and just recently, he received a notice from SSA cutting his benefits due to income reported for 2016 in which the taxpayer had no income. The employee reviews the account and finds no prior identity theft indicators have been applied. The employee will input a TC 971 AC 522 PNDCLM initiating an identity theft case for both the 2015 and 2016 tax years.

- (2) If, at the time of case closure you find the Entity module has not been flagged with a TC 971 AC 522 PNDCLM/UNWORK, do not input this code at closing. Close the identity theft issue with TC 971 AC 50X, as appropriate. Applying TC 971 AC 522 PNDCLM/UNWORK at case closure serves no purpose.

Exception: If you have determined there was no tax-related identity theft (NOIDT), you must enter a TC 971 AC 522 UNWORK so it can be reversed with a TC 972 AC 522 NOIDT. The TC 972 must be post-delayed one week to allow the TC 971 to post.

- (3) When a taxpayer asserts tax-related identity theft, request the taxpayer provide an identity theft claim. See IRM 25.23.2.3, *Identity Theft Claims - General Guidelines*. When that claim is received, the employee will input a TC 971 AC 522 UNWORK.

Caution: When a taxpayer files a return with an identity theft claim attached, Submission Processing (SP) Code and Edit employees will edit an SPC 8 on the paper return. The SPC 8 is transcribed and generates a TC 971 AC 522 WI SP UNWORK. Beginning in 2014, the SPC 8 will generate an acknowledgement letter advising the taxpayer that the Service received his/her claim. Refer to IRM 25.23.2.3, *Identity Theft Claims - General Guidelines*.

- (4) If an employee receives a call from a taxpayer, stating his e-file return was rejected because of a previously used Primary or Secondary TIN, the employee can attempt to stop the refund. Employees only have two or three days to stop a refund. The CSR must first do high risk disclosure and then follow IRM 21.4.1.5.7.1, *Direct Deposit of Refunds*. Input TC 971 AC 522 PNDCLM if not already on the account. See IRM 25.23.2.4.4, *Initial Allegation or Suspicion of Tax-Related Identity Theft - Identity Theft Indicators*, for codes and additional information. For information on stopping the refund, see IRM 21.4.1.5.10, *Refund Intercept Command Code NOREF with Definer "P"*.
- (5) There will be only one TC 971 AC 522 PNDCLM per tax year on the entity module.

Example: Taxpayer calls IRS on May 15, 2017, claiming to be a victim of identity theft for a 2015 audit assessment. The employee requests the taxpayer respond to the examination with an identity theft claim and applies the TC 971 522 PNDCLM to the 2015 account. On September 12, 2017, the taxpayer calls IRS claiming to be a victim of identity theft for the same 2015 audit assessment. The CSR reviews the account and finds there is no open IDRS controls and there is an un-reversed 522 PNDCLM. The CSR will follow normal IRM procedures for resolving the call. The CSR will not input another 522 PNDCLM as one is already present on the entity.

- (6) Do not input more than one TC 971 AC 522 PNDCLM per tax year on the module. If, however the taxpayer is reporting identity theft and the account reflects a reversed AC 522 PNDCLM, a new TC 971 AC 522 PNDCLM will be appropriate.

Example: A taxpayer alleging identity theft contacted IRS on February 2, 2017 regarding tax year 2015. The employee requested an Identity Theft claim from the taxpayer. On May 1, 2017, the employee input a TC 972 AC 522 NORPLY as the taxpayer did not provide the claim and/or any additional information requested. On June 3, 2017, the taxpayer provided the claim and/or requested information. The employee input a TC 971 AC 522 UNWORK to reflect receipt of a claim.

25.23.2.4.4.2
(09-15-2020)

Mass Input of Identity Theft Tracking Indicators

- (1) Identity theft tracking indicators are used to mark both tax-related and non-tax-related incidents of identity theft. The indicators help IRS in identifying open and closed cases. Generally, indicators are input to taxpayer accounts using IDRS. However, under certain conditions, the service may consider marking many accounts with specific identity theft indicators at one time by posting the indicator directly to Masterfile.
- (2) Functions considering this path for marking accounts **MUST** first contact IPSO Technical Staff via e-mail for IPSO concurrence. The e-mail must contain the following:
 - A detailed explanation of why the indicator is being used to mass flag accounts.
 - The number of accounts being marked with an identity theft indicator.
 - The method by which taxpayers will be notified that an indicator was placed on their account and an example of that notification letter or notice.
 - A draft of the function's IRM guidance, IPU, or SERP alert detailing the marking of the accounts and the date the guidance will be available.
 - An agreement with the unpostable functions that will resolve subsequent unpostable conditions resulting from the mass indicator inputs.

Direct the E-mail to the following mailbox: ipp@irs.gov.

- (3) Any efforts to post identity theft indicators directly to Masterfile **MUST** use the formats established in Exhibit 25.23.2-2 through Exhibit 25.23.2-15. Not following the specifications for input will negatively affect the ability to reverse or take corrective actions. Failure to adhere to established formats will impede or prevent the business rules tied to the indicators from functioning as intended.

25.23.2.4.5
(10-02-2023)

IRS Initiated Suspicion of Identity Theft - TC 971 AC 522 IRSID

- (1) In situations where the IRS suspects identity theft may have occurred, employees will mark the entity account, using Command Code (CC) REQ77 initiated from ENMOD to input a TC 971 AC 522 reflecting a Tax Administration Source Code IRSID, and the tax year of the identity theft incident if no TC 971 AC 522 PNDCLM, UNWORK or IRSID already exists. See Exhibit 25.23.2-10, *IMF Only TC 971 AC 522 Tax-Related Identity Theft, Case Status (Initial Claim/ Suspicion)*, for additional information.

Note: If the allegation or suspicion of IDT is for an Economic Impact Payment (EIP), check the TC 971 AC 199 on IMFOLE to see the source of the EIP. If the source is a 2018 return, input 2018 as the tax year affected by IDT. If the source is something other than a 2018 return, input 2019 or 2020 as the tax year affected.

Reminder: If you suspect identity theft on more than one tax year, input TC 971 AC 522 IRSID for each tax year affected by identity theft, as appropriate. If a TC 971 AC 522 PNDCLM (Taxpayer self-identified) UNWORK (claim received) or IRSID already exists for that tax year, do not apply another.

- (2) Apply the TC 971 AC 522 IRSID when you initially suspect ID theft may have occurred. Post filing Compliance programs should not enter TC 971 AC 522

IRSID until after the taxpayer has had an opportunity to respond to the IRS notice/letter, unless there is clear evidence that leads you to suspect identity theft.

Reminder: If there is already an unreversed TC 971 AC 522 IRSID, UNWORK or PNDCLM for the affected tax year, do NOT input TC 971 AC 522 IRSID.

- (3) The Secondary Date field on CC REQ77 is limited to the current calendar year (cannot be the current day or any future date) and 7 prior years. The secondary date field will not allow the input of any date outside that range. See IRM 25.23.2.3.8.1, *Command Code REQ77 Secondary Date and Old Case Year Issue* for more information.
- (4) Do not input more than one TC 971 AC 522 IRSID per tax year on the entity module.

Example: Accounts Management, while working a duplicate filing condition for the 2015 tax year, suspects an identity theft incident may have occurred. The TC 976 return appears to have been filed by the SSN owner at the address of record for many years. The TC 150 reflects income not supported by IRPTR, suspicious dependents and a different address from prior year filings. The CSR will review ENMOD/IMFOLE for an unreversed TC 971 PNDCLM, UNWORK or IRSID. If none are present, the CSR will input a TC 971 AC 522 IRSID initiating an identity theft case and follow their IRM procedures to resolve their case. If ID theft is suspected in an additional tax year, a TC 971 AC 522 IRSID will be applied for each tax year suspected of involving identity theft.

- (5) IPSO considers an account with a TC 971 AC 522 IRSID and no subsequent TC 971 AC 506 (indicating a completely resolved account) an open identity theft case. Subsequently, if the case is deemed NOT to be identity theft, the assigned employee will document the decision in a CII Case Note and reverse the TC 971 AC 522 IRSID with a TC 972 AC 522 IRSERR.
- (6) If, at the time of case closure you find the Entity module has not been flagged with a TC 971 AC 522 IRSID, do not input this code at closing. Close the identity theft issue with a TC 971 AC 506.

Exception: If you have determined there was no tax-related identity theft (NOIDT), document the decision in a CII Case Note and do not input any closing indicators on the Entity module. See IRM 25.23.2.6 (5), **Closing Identity Theft Issues**.

25.23.2.5 (03-16-2023) Statute Protection

- (1) A statute of limitation is a time period established by law to review, analyze and resolve taxpayer and/or IRS tax related issues.
- (2) The Internal Revenue Code (IRC) requires that the IRS will assess, refund, credit, and collect taxes within specific time limits. These limits are known as the Statutes of Limitations. When they expire, the IRS can no longer assess additional tax, allow a claim for refund by the taxpayer, or take collection action. The determination of Statute expiration differs for Assessment, Refund, and Collection.

- (3) Follow IRM 25.6.1, *Statute of Limitations Processes and Procedures*, to ensure all statutes are protected.
- (4) A case is considered imminent when a tax increase is required and it is within 180 days of the **valid** TC 150, TC 976/TC 977 or unprocessed return.

Note: Invalid returns meeting streamline processing criteria do not require statute protection; however, other returns on the account may. Each return must be considered separately.

- (5) When a tax increase for a TC 976/977 return is imminent but more than 90 days remain before the ASED expires, a normal adjustment may be input on IDRS.

Example: The determination for a tax year 2019 module is Invalid/Valid with a lost refund. The invalid return meets nullity criteria, and the valid return was timely filed. The ASED for the valid return is April 15, 2023. If working the case on January 6, 2023, a quick assessment is not required. The account may be adjusted using TC 290 input with IDRS CC REQ54.

- (6) To prevent a barred statute assessment, a quick assessment is required when:
 - a. The ASED on the CN account will expire in 90 days or less or
 - b. The ASED on the IRSN account will expire in 180 days or less.
- (7) When a quick assessment is needed, complete the following:
 - a. Verify the statute dates for the return in question.
 - b. Edit the return with the correct tax.
 - c. Determine the amount of tax currently on the account.
 - d. Calculate the amount of the tax increase.
 - e. Complete the Form 2859, Request for Quick or Prompt Assessment.

Note: A quick assessment must be approved by the manager.

- (8) When the invalid return requires an IRSN and is statute imminent, follow procedures in IRM 25.23.2.5.1, *Statute Protection – Single Return*.

25.23.2.5.1 (03-16-2023) Statute Protection - Single Return

- (1) Review IDRS to verify:
 - No TC 976/977 transactions are on the module.
 - There are no unnumbered unprocessed returns received from the valid taxpayer in the case documents.
 - The valid taxpayer's return was not moved to MFT 32 in error.

Caution: IDTVA employees must search CII for related cases. If related cases are found, review the case documents in each to verify there are no unnumbered unprocessed returns from the valid taxpayer.

- (2) No action is required to protect the CN module when there is **no**:
 - TC 976/977 return
 - Unprocessed return, or

25.23 Identity Protection and Victim Assistance

- Valid return moved to MFT 32 (when there is no TC 150 present on MFT 30)

Note: Determine if the invalid TC 150 must be moved. Refer to IRM 25.23.4.9.1, *Determining When Specific Year Account Information Must Be Moved*, and its subsections for additional information.

- (3) If less than 180 days remain before the expiration of the ASER for the invalid return being moved to an IRSN, the IRSN module must be protected. Prepare Form 2859, Request for Quick or Prompt Assessment. Annotate at the top of the form "ID Theft Statute Year".

Note: An example for completing Form 2859 can be found on the *IDTVA Hub*.

- a. The Form 2859 will be prepared for the correct amount to protect any tax increase on the IRSN module. Input the assessment amount as a TC 150 on Form 2859. Input the following in the Remarks section: "Agreed assessment. Do not bill the taxpayer. Send no notices to the taxpayer. The TC 150 will be nullified or moved to an IRSN".
 - b. **Do not include any tax decrease or credit increase adjustments to the account.**
 - c. In Part B, Requestor Information, input the name and campus preparing the document.
- (4) Prepare Form 3210, Document Transmittal. Fax the Form 3210, Form 2859, and the statute return to the applicable Accounting office. Attach the Form 2859 to your CII case.
 - (5) Update the control base to the employee requesting the quick assessment and use activity code "QUICK2859".

Note: If suspending the case, update the activity code **after** the case has been suspended.

- (6) Keep a copy of the SSN owner's return and Form 2859 with documentation for monitoring.
- (7) Complete credit transactions and transfers of excess funds **after** the Form 2859 has been processed and the assessment has posted.
- (8) If there is a TC 976/977 return, unprocessed return, or valid return moved to MFT 32 (when there is a posted TC 150 on MFT 30), follow procedures in IRM 25.23.2.5.2, *Statute Protection - Multiple Returns*, or IRM 25.23.2.5.3, *Statute Protection - Multiple Returns and MFT 32*.

25.23.2.5.2 (03-16-2023) Statute Protection - Multiple Returns

- (1) The procedures below apply to cases with multiple returns received and a TC 150 posted on the MFT 30 module for the CN. If the multiple return was moved to MFT 32 in error, refer to IRM 25.23.2.5.3, *Statute Protection - Multiple Returns and MFT 32*.
- (2) Determine the IRS received date of the taxpayer's return. If it was filed on or before the return due date, it is considered timely filed.

Exception: If an extension was filed, the taxpayer has until the extended due date.

- (3) Determine the ASED of the taxpayer's return – add 3 years to the received date.
- (4) If the ASED is within 180 days of expiring, it is considered a STATUTE return.

Reminder: When a tax increase for a TC 976/977 return is imminent but more than 90 days remain before the ASED expires, a normal adjustment may be input on IDRS.

Example: 2019 return is due 04/15/2020. The ASED is 04/15/2023. The case would be considered a statute case as of October 15, 2022.

- (5) Compare the account, including adjustments, to determine if all assessments match the valid return figures.
- (6) If 90 days or less remain before expiration of the valid ASED, and the CN module requires a tax increase or credit decrease, prepare Form 2859, Request for Quick or Prompt Assessment. Annotate at the top of the form "ID Theft Statute Year".

Note: An example for completing Form 2859 can be found on the *IDTVA Hub*.

- a. The Form 2859 will be prepared for the correct amount to protect any tax increase and credit decreases to the account based on the taxpayer's return. Input the assessment amount as a TC 290 on Form 2859. Input the following in the Remarks section: "Agreed Assessment. Do not bill the taxpayer. Send no notices to the taxpayer. The TC 150 will be nullified or moved to an IRSN".
 - b. **Do not include any tax decrease or credit increase adjustments to the account.**
 - c. In Part B, Requestor Information, input the name and campus preparing the document.
- (7) Prepare Form 3210, Document Transmittal. Fax the Form 3210, Form 2859 and the statute return to the applicable Accounting office. Attach the Form 2859 to your CII case.
 - (8) Update the control base to the employee requesting the quick assessment and use activity code "QUICK2859".

Note: If suspending the case, update the activity code **after** the case has been suspended.

- (9) Keep a copy of the SSN owner's return and Form 2859 with documentation for monitoring.
- (10) Do not make any adjustments to credit transactions on the account.
- (11) Complete credit transactions and transfers of excess funds **after** the Form 2859 has been processed and the assessment has posted. .

25.23.2.5.3
(03-16-2023)

**Statute Protection -
Multiple Returns and
MFT 32**

- (1) The procedures below apply to cases with multiple returns received with the valid return moved to MFT 32 in error.
- (2) If a TC 150 is not present on the MFT 30 module, do not request a quick assessment. Follow procedures in paragraph (3) of IRM 25.23.4.15, *MFT 32 Cases – Moved in Error*, to refer the case to RIVO statutes for resolution.
- (3) If a TC 150 is present on the MFT 30 module, continue with the procedures below to protect the account.
- (4) Determine the IRS received date of the valid taxpayer's return. If it was filed on or before the return due date, it is considered timely filed.

Exception: If an extension was filed, the taxpayer has until the extended due date.

- (5) Determine the ASED of the valid taxpayer's return - add 3 years to the received date.
- (6) If the ASED is within 180 days of expiring, it is considered a STATUTE return.

Reminder: When a tax increase for a TC 976/977 return is imminent but more than 90 days remain before the ASED expires, a normal adjustment may be input on IDRS.

Example: 2022 return is due 04/18/2023. The ASED is 04/18/2026. The case must be considered a statute case as of October 18, 2025.

- (7) Compare the account, including adjustments, to determine if the tax and credits match the valid return figures.
- (8) If 90 days or less remain before expiration of the valid ASED, and the CN module requires a tax increase or credit decrease, prepare Form 2859, Request for Quick or Prompt Assessment, annotate at the top of the form "ID Theft Statute Year".

Note: An example for completing Form 2859 can be found on the *IDTVA Hub*.

- a. The Form 2859 will be prepared for the correct amount to protect any tax increase and credit decreases to the account based on the valid taxpayer's return. Input the assessment amount as a TC 290 on Form 2859. Input the following in the Remarks section: "Agreed Assessment. Do not bill the taxpayer. Send no notices to the taxpayer. The TC 150 will be nullified or moved to an IRSN".
- b. **Do not include any tax decrease or credit increase adjustments to the account.**
- c. In Part B, Requestor Information, input the name and campus preparing the document.
- (9) Prepare Form 3210, Document Transmittal. Fax both forms and the statute return to the applicable Accounting office. Attach the Form 2859 to your CII case.
- (10) Update the control base to the employee requesting the prompt assessment and use activity code "Quick2859".

Note: If suspending the case, update the activity code **after** the case has been suspended.

- (11) Keep a copy of the SSN owner's return and Form 2859 with documentation for monitoring.
- (12) Do not make any adjustments to credit transactions on the account.
- (13) Complete credit transactions and transfers of excess funds **after** the Form 2859 has been processed and the assessment has posted.

25.23.2.5.4 (09-06-2023) Barred Statutes

- (1) These procedures are for those responsible for filling out the barred report and outlining the statute unit's role in the process. Refer to IRM 25.23.4.9.3 *Addressing Barred Assessments on Identity Theft (IDT) Cases*, for instructions to resolve a barred account. When working IDT cases and it is determined an ASED has expired and an assessment cannot be made, the case must be written up as a barred assessment, unless the barred amount is within tolerance. Refer to IRM 25.6.1.13.2.4, *Identifying Barred Statute Cases*, for examples of **barred assessments** and tolerance amounts.

Note: When the barred amount is within tolerance, the report is not required. TC 971 AC 090 is input on the module to identify the barred assessment under the tolerance level. Refer to IRM 25.6.1.9.15, *Assessment Tolerance Level*, for additional information.

- (2) Cases that are barred with ID Theft involvement must be resolved by an ID Theft employee. After the actions have posted to the account, the case will be referred to the local statute function for the completion of Form 9355, Barred Statute Report.

Exception: IDTVA will complete Form 9355, Barred Statute Report, and forward a complete packet to the local statutes unit. See IRM 25.23.4.9.3.1, *Adjusting Accounts with Barred Assessments*, for additional information.

- (3) The Statute Function will:
 1. Prepare original and two copies of Form 9355.
 2. Assign the case a control number.
 3. Establish an IDRS control base using category "BARD". The category BARD cases must be processed within 99 calendar days of the case establishment date as stated in IRM 3.30.123.5.8(4), *Statutes*.
 4. Complete all remaining actions as required per IRM 25.6.1.13.2.6, *Routing and Controlling Form 9355*.

25.23.2.6 (09-06-2023) Closing Identity Theft Issues

- (1) Prior to closing the identity theft case take the following actions: **Actions include, but are not limited to:**

- Release notice or enforcement holds, as appropriate
- Address all refund situations, as appropriate
- Verify and correct the taxpayer's address, as appropriate

Reminder: If the secondary taxpayer is determined to be a victim of identity theft, you **MUST** update the address on the secondary's entity module

25.23 Identity Protection and Victim Assistance

- Refer issues identified during case closure analysis to another function, ONLY when you cannot resolve the case within your own function
- Address balances due and restore Installment Agreements (IAs) and Currently Not Collectable (CNC) as appropriate

Note: See IRM 25.23.4.12.1, *Collection Activity – Form 14394* and IRM 25.23.4.12.2, *Collection Activity – Form 13794 Additional Actions Required - Lien*.

Reminder: Specialty Resolution functions Exam and AUR do not re-instate IA. F14394 will be sent back to Specialty Resolution ACSS) to re-instate.

- Address offsets and restore credit elect, as appropriate
- Adjust the account to the taxpayer's figures, and
- Advise the taxpayer of actions taken

Caution: The importance of updating the address prior to inputting the TC 971 AC 501/506 cannot be stressed enough. If the address is not updated appropriately, **including an update for both the Primary and Secondary taxpayer's entities**, the victim notification letter will go to the wrong address. In addition, failure to follow the appropriate sequence could result in the Identity Protection Personal Identification Number (IP PIN) being sent to the ID thief instead of the ID theft victim. Refer to IRM 25.23.2.9, *Identity Protection Personal Identification Number (IP PIN)*.

Reminder: Use a post delay on other transactions when changing the taxpayer's address.

Reminder: Identity Theft indicators AC 501, AC 504, AC 505, AC 506, AC 522, AC 523, AC 524 and AC 525 never expire. In addition, once a taxpayer is in the IP PIN population, they cannot be removed.

- (2) The TC 971 AC 501/506 cannot be input until the taxpayer is no longer harmed by identity theft issues impacting tax administration. The TC 971 AC 501/506 indicates all identity theft tax administration issues have been resolved from the taxpayer's perspective.

Example: An identity thief's return posted to the victim's 2015 account first. The victim was expecting a refund for 2015. In 2012, the victim was assessed by exam for underreporting income originating from the identity theft. The victim did not have a filing requirement in 2012. Prior to marking ENMOD with a TC 971 AC 501 for the 2012/2015 tax year, the employee assigned MUST:

VERIFY- the victim's address has been verified and updated on ENMOD
ADJUST- Input adjustments, as appropriate

- (3) A case control **must** be maintained until the identity theft case is resolved.
- (4) The employee assigned the case will close the identity theft issue by marking the account with the appropriate identity theft indicator. When the taxpayer has been determined to be a victim of tax related identity theft, these action codes (501 and 506) provide the taxpayer protection against future occurrences of identity theft.

- (5) At case closure if the Entity module has not been flagged with a TC 971 AC 522 PNDCLM/UNWORK/IRSID;
 - a. If tax-related IDT determined, do not input any AC 522s, close with TC 971 AC 50X as appropriate.
 - b. If non tax-related IDT, do not input any AC 522s, close with TC 971 AC 504.
 - c. If no tax-related identity theft (NOIDT) and **TP initiated**, you must enter a TC 971 AC 522 UNWORK so it can be reversed with a TC 972 AC 522 NOIDT.
 - d. If no tax-related identity theft (NOIDT) and **IRS Initiated**, you must enter a TC 971 AC 522 IRSID so it can be reversed with a TC 972 AC 522 IRSERR.

25.23.2.6.1
(09-06-2023)
**Closing Taxpayer
Initiated Identity Theft
Affecting Tax
Administration - TC 971
AC 501**

- (1) To indicate resolution of a taxpayer initiated identity theft claim, mark the victim's account using Command Code (CC) REQ77 initiated from ENMOD, to input a TC 971 AC 501 reflecting an appropriate Tax Administration Source Code depending upon the facts and circumstances of the case along with the tax year of the identity theft incident. The AC 501 is applied to a taxpayer's account when **all** of the following occur:

- a. The identity theft incident was taxpayer initiated, or the identity theft incident was IRS determined but additional taxpayer information was required to resolve all issues.
- b. All corrective actions have been taken. This includes verifying and updating the taxpayer's address on ENMOD, as applicable.

Caution: Marking the account with AC 501 prior to correcting the victim's address may result in the issuance of the victim notification letter to an incorrect address and may allow an identity thief's return to post while the legitimate taxpayer's return will unpost.

- c. There must be a tax-related impact to affect tax administration. This includes years in retention.

- d. **Complete Case Analysis (CCA):** Perform CCA to ensure all identity theft related issues have been addressed and resolved. This includes all outstanding TC 971 AC 522s. Refer to IRM 25.23.2.6, *Closing Identity Theft Issues*.

Note: Close years identified by the Taxpayer using TC 971 AC 501. Close additional years identified through CCA with TC 971 AC 501 with MISC **REFCCA** for refund related determinations and **ICMCCA** for income related determinations impacting tax administration.

#

25.23 Identity Protection and Victim Assistance

- e. **Verify Taxpayer Address:** Verifying and updating the taxpayer's address **MUST** be done before inputting the TC 971 AC 501.

Reminder: Use a post delay on other transactions when changing the taxpayer's address to prevent notices from generating to the identity thief.

- f. Follow functional case closing guidance, as appropriate.

- (2) TC 971 AC 501 can be input by any business unit delegated the authority and programmed to use this code when closing identity theft issues.

Caution: Do not enter another TC 971 AC 501 if there is an existing AC 501 for the year affected. This will cause an Unpostable condition.

Note: For additional information on TC 971 AC 501 refer to Exhibit 25.23.2-2, *IMF Only TC 971 AC 501 — Taxpayer Initiated Identity Theft Case Closure (Tax-Related)*.

- (3) If more than one year is affected by identity theft and resolved, the employee will enter the corresponding TC 971 AC 501 for each year listed by the taxpayer and TC 971 AC 501 with MISC **REFCCA (Refund Related) or ICMCCA (Income Related affecting tax administration)** for additional impacted years identified by CCA.

Reminder: If, at the time of case closure you find the Entity module has not been flagged with a TC 971 AC 522 PNDCLM/UNWORK/IRSID, do not input this code at closing. Close the identity theft issue with TC 971 AC 50X, as appropriate.

- (4) The Secondary Date field on CC REQ77 is limited to the current calendar year (cannot be the current day or any future date) and 7 prior years. The secondary date field will not allow the input of any date outside that range. See IRM 25.23.2.3.8.1, *Command Code REQ77 Secondary Date and Old Case Year Issue* for more information.

25.23.2.6.1.1
(09-15-2020)

Systemic Actions Taken After TC 971 AC 501 Placed on Account

- (1) Notice CP 01, Identity Theft Claim Acknowledgment, is used for victim notification on identity theft issues closed with a TC 971 AC 501. CP 01 systemically generates two posting cycles after the TC 971 AC 501 is input, depending upon when the taxpayer's account adjustment is completed. **The CP 01 is issued only once within a three-year period.**

Note: See IRM 25.23.2.4.1, *Tracking and Reporting Identity Theft Cases - Identity Theft Indicators*, for details on when an IP PIN will be issued and the method for issuance

CP 01 contains the following information:

- a. Confirmation that any requested additional information was received and accepted
- b. Information about how the IRS will monitor the taxpayer's account and income tax returns
- c. Information about identity theft prevention and available identity theft-related resources

Note: Letter 4445 C, Acknowledgement Notification, was previously used for victim notification for TC 971 AC 501s input through June 30, 2009. Letter 4445 C may be used in those instances where taxpayers indicate they never received Notice CP 01.

Note: A Notice CP 01 is not applicable to, and does not systemically generate, when a TC 971 AC 506 is applied to a taxpayer's account.

- (2) The taxpayer should continue to file tax returns each tax year, as appropriate.
- (3) The presence and date of the TC 971 AC 501 on an account will be used as a data point, along with other key information, to make case-related decisions. The existence of the identity theft indicator will not supersede or replace existing procedures for case resolution.

#

25.23.2.6.2 (10-01-2024) Manually Reversing TC 971 AC 501

- (1) In some instances, it may be necessary to manually reverse TC 971 AC 501. Reversal may be necessary because of any of the following reasons:
 - a. **TPRQ** - The taxpayer requests reversal.
 - b. **IRSERR** - There was a keying or internal error in the input of the TC 971 AC 501.
 - c. **FALSE** - RESERVED
 - d. **IRSADM** - The TC 971 AC 501 has an internally identified negative affect on the taxpayer. For example, a programming issue.
 - e. **OTHER** - There are other reasonable circumstances not listed above.

Note: Be sure to select the correct code. If codes a-d above are not applicable, use OTHER. Refer to Exhibit 25.23.2-3, *IMF Only TC 972 AC 501 - Reversal of TC 971 AC 501*, for additional information.

Caution: If the year in question being reversed is older than the current calendar year minus 7 years, CC REQ77 will not accept the year. See 25.23.2.3.8.1 Command Code REQ77 Secondary Date and Old Case Year Issue for more information.

- (2) Actions needed prior to manually reversing an identity theft marker at the taxpayer's request:
 - 1. If this is a telephonic request, be certain that you are speaking with the taxpayer. Inadequate authentication of the identity of a caller could result in an unauthorized disclosure of return or return information. Refer to IRM 21.1.3.2.3, *Required Taxpayer Authentication*, and IRM 21.1.3.2.4, *Additional Taxpayer Authentication*.
 - 2. Ask probing questions to determine why the taxpayer is requesting indicator removal and document AMS, or the case history if you do not have access to AMS, with the taxpayer's response. For example, "Can you provide the reason why you would like this protection removed from your account?"

3. Explain to the taxpayer the indicator will:
Help prevent future identity theft incidents
Ensure any returns filed are reviewed for identity theft indications
Include the issuance of an IP PIN for as long as the indicator remains active
4. If the taxpayer insists on removal of the identity theft indicator after you have explained the benefits, review the account to determine if the identity theft issue is open in another function. If there is an open identity theft case, refer the case to that function using your normal referral procedures. Do not take actions on identity theft cases being worked by another function.

25.23.2.6.3
(10-01-2024)

**Closing IRS Determined
Identity Theft Affecting
Tax Administration - TC
971 AC 506**

- (1) To indicate resolution of an IRS determined identity theft case a TC 971 AC 506 is applied to a taxpayer's account when the incident affects tax administration. Such incidents can result from any of the following:
 - Phishing
 - Refund schemes
 - Verified false returns
 - Duplicate filing research
 - Certain unpostable returns
- (2) Prior to marking the taxpayer's account with a TC 971 AC 506 the function **MUST** ensure all corrective actions have been taken which includes:
 - a. Verifying and updating the taxpayer's address on ENMOD, as applicable.
Caution: Marking the account with AC 506 prior to correcting the victim's address may result in negative consequences for the victim. Letters and notices regarding the IP PIN may be directed to an incorrect address.

Reminder: Use a post delay on other transactions when changing the taxpayer's address to prevent notices from generating to the identity thief.
 - b. Advising the taxpayer of actions taken.
 - c. Issuing the taxpayer's correct refund.
 - d. Adjusting the account to the taxpayer's figures.
- (3) Marking an account with TC 971 AC 506 will not generate a notice to the taxpayer regarding the resolved identity theft issue. The function that inputs the TC 971 AC 506 will notify the taxpayer (victim), by letter, that someone may have attempted to use his or her SSN. This victim notification letter will include:
 - Information about identity theft prevention
 - Information about identity theft related resources
 - Information about the identity theft indicator placed on his or her account.

Caution: If the TC 971 AC 506 is not input prior to cycle 47 of the processing year (meaning an IP PIN/CP01A will **not** generate for the upcoming filing season) do not include the sentences "To further protect you, we will issue you an IP PIN by mail in December. You will need an identity protection PIN to file your tax returns in the future" as no IP PIN will be issued.

Reminder: The IP PIN will generate annually for as long as the indicator remains active.

Reminder: If, at the time of case closure you find the Entity module has not been flagged with a TC 971 AC 522 PNDCLM/UNWORK/IRSID, do not input this code at closing. Close the identity theft issue with TC 971 AC 50X, as appropriate.

Input of a TC 971 AC 506 does not generate a systemic notification to the taxpayer. To notify the taxpayer of actions taken to resolve identity theft issues, the Letter 4310 C or another appropriate letter may be used.

#

- (5) In some instances, it may be necessary to manually reverse TC 971 AC 506. If reversal (TC 972 AC 506) is indicated, see Exhibit 25.23.2-9, *IMF Only TC 972 AC 506 Tax-Related, Reversal of Identity Theft Case Closure, IRS Identified*, for a description of reasons for the reversal.
- (6) To indicate resolution of an IRS determined Identity Theft Case involving tax administration, mark the victim's account using Command Code (CC) REQ77 initiated from ENMOD to input a TC 971 AC 506 reflecting an appropriate Tax Administration Source Code depending upon the facts and circumstances of the case along with the tax year of the identity theft incident. The TC 971 AC 506 is applied to a taxpayer's account when **all** of the following occur:

- a. **All** corrective actions have been taken. This includes verifying and updating the taxpayer's address on ENMOD.

Caution: If you do not have a valid address for the taxpayer, use the Service Center address to prevent an IP PIN from going to incorrect taxpayer. Refer to IRM 3.13.5.66, *Campus Address Used Only When Taxpayer Address is Unavailable*.

- b. The taxpayer's identity theft issue affects tax administration.
- c. Perform **complete case analysis** to ensure all identity theft related issues have been addressed and resolved. This includes all outstanding TC 971 AC 522s. See IRM 25.23.2.6, *Closing Identity Theft Issues*.

- (7) The procedural guidance for your functional area must be followed as to when the TC 971 AC 506 should be input. Your procedural guidance, however, must adhere to the guidelines provided in this subsection.
- (8) The Secondary Date field on CC REQ77 is limited to the current calendar year (cannot be the current day or any future date) and 7 prior years. The secondary date field will not allow the input of any date outside that range. See IRM 25.23.2.3.8.1, *Command Code REQ77 Secondary Date and Old Case Year Issue* for more information.
- (9) Generally, there should be only one TC 971 AC 506 per tax year. However, some automated systems are not programmed to look for an existing TC 971 AC 506 for a specified tax year and in those instances, the automated system may have applied a second AC 506 to the account. While automated systems may apply a second Identity Theft indicator for a specific year, manual input is limited to one AC 506 per tax year.

Exception: Accounts that meet the criterion described in IRM 25.25.2.10, *Special Procedures for Returns Previously Identified as Identity Theft Returns*, where a good taxpayer return was received on an account formerly flagged with TC 971 AC 506 OMM may reflect more than one AC 506 of the same year. Refer to IRM 25.25.2.11, *Identity Theft Scheme Criteria*, for additional information.

If you receive Form 14039 and find the taxpayer's entity for the years in question have already been flagged with AC 506, apply an AC 501 for the impacted tax years.

Exception: Taxpayers involved in a **Data Breach** will have an additional TC 971 AC 506 present on their account as indicated below. The application of the "TC 971 AC 506 WI AM OTHER", ensures these taxpayers will receive a CP 01A providing them an IP PIN. See IRM 25.23.2.8.6, *Disabled Online Accounts TC 971 AC 527*, for more information

25.23.2.6.4 (10-01-2024)

Manually Reversing TC 971 AC 506

- (1) In some instances, it may be necessary to manually reverse TC 971 AC 506. Reversal may be necessary because of any of the following reasons:
 - a. **TPRQ-** The taxpayer requests reversal.
 - b. **IRSERR-** There was a keying or internal error in the input of the TC 971 AC 506 or IRS determined possible identity theft (IRSID) and later determined no identity theft occurred.
 - c. **FALSE-Reserved**
 - d. **IRSADM-** The TC 971 AC 506 has an internally identified negative affect on the taxpayer. For example, a programming issue.
 - e. **OTHER-** There are other reasonable circumstances not listed above.

Note: Be sure to select the correct code. If codes a-d above are not applicable, use OTHER.

Caution: If the year in question being reversed is older than the current calendar year minus 7 years, CC REQ77 will not accept the year. See IRM 25.23.2.3.8.1, *Command Code REQ77 Secondary Date and Old Case Year Issue* for more information.

- (2) Actions needed prior to manually reversing an identity theft marker at the taxpayer's request:
 1. If this is a telephonic request, be certain that you are speaking with the taxpayer. Inadequate authentication of the identity of a caller could result in an unauthorized disclosure of return or account information. Refer to IRM 21.1.3.2.3, *Required Taxpayer Authentication*, and IRM 21.1.3.2.4, *Additional Taxpayer Authentication*.
 2. Ask probing questions to determine why the taxpayer is requesting Action Code removal and document AMS or the case history if you do not have access to AMS with the taxpayer's response. For example, "Can you provide the reason you would like this protection removed from your account?"
- (3) Explain to the taxpayer that the AC 506 will:
 - Help prevent future identity theft incidents
 - Ensure any returns filed are reviewed for identity theft indications
 - Include the issuance of an IP PIN for as long as the IP PIN indicator remains active
- (4) If the taxpayer insists on removal of the identity theft indicator after you have explained the benefits, review the account to determine if the identity theft issue is open in another function. If there is an open identity theft case, refer the case to that function using your normal referral procedures. Do not take actions on identity theft cases being worked by another function. If there is no open IDRS control, review the Miscellaneous Field Code to determine what function applied the AC 506. Refer the case using your normal procedures to that function. The function that applied the AC 506 will determine if the 506 will be reversed.

Note: When referring a case to another function for AC 506 removal be sure to inform the taxpayer that the case is being referred to another function using your normal procedures for case referral.

25.23.2.6.5
(04-29-2020)
Closing Identity Theft Cases with Tax Delinquency Inquiries (TDI)

- (1) Take these actions when a taxpayer submits a Form 14039 alleging identity theft and he/she does not have a filing requirement. If the Identity Theft allegation is confirmed and includes a tax module in Masterfile status 02 or 03, input a TC 590 cc 020. This action will remove the account from the TDI inventory. Continue to correct the account as needed. Conduct research to determine if any modules in status 02 or 03 must be closed because the taxpayer has no filing requirement.

Example: A taxpayer alleges identity theft on a 2012 tax year stating he/she has no filing requirement. The allegation is confirmed and the 2012 account is cleaned up. However, the 2013 account is in Masterfile status 02 or 03 where a Tax Delinquency Inquiry (TDI) notice was issued. The case-worker researches account information for tax year 2013 and determines the taxpayer is not liable to file or the taxpayer states/verifies there is no filing requirement for tax year 2013. Inputting a TC 590 cc 020 on the 2013 account will remove the account from the TDI inventory.

- (2) Take these actions when a taxpayer submits a Form 14039 alleging identity theft and he/she does not have a filing requirement, and there is a TC 594 (indicating a joint return was filed with the spouse as primary). If the Identity Theft allegation is confirmed, input a TC 592 to reverse the TC 594, wait one cycle and input a TC 590 cc 020. This is necessary because IDRS CC FRM49 does not accept posting delay codes. This will prevent erroneous generation of TDI notices.

Example: A Guam taxpayer was a victim of identity theft on a tax year 2012 Married Filing Joint (MFJ) tax return. The taxpayer was used as the secondary filer (spouse). The taxpayer does not have a U.S. filing requirement as he/she filed and paid all taxes to Guam. It appears when the fraudulent prior year return was backed off the account and the MFJ indicator (TC 594-84) was reversed (TC 592) on his/her account, within a few cycles a TDI erroneously generates requesting a return from the victim (who believes his/her account was resolved). A review of IRP on the affected accounts reflects all income was earned in Guam and no prior year returns were ever requested by TDI.

Example: A taxpayer was a victim of identity theft on a tax year 2013 Married Filing Joint (MFJ) tax return. The taxpayer was listed as the secondary filer (spouse) and TC 594 posted to the victim's 2013 tax module with a cross reference to an erroneous SSN. To reverse the erroneous TC 594, input transaction code 592, wait one week, then input TC 590 cc 020. The TC 592 must post prior to the TC 590 or the account will be in TDI status.

- (3) If an identity theft allegation is confirmed and includes a tax module in Master-file status 02 or 03, take these actions when a taxpayer submits correspondence that includes an unprocessed return.

Note: If the IDT TP has filing requirements and **DOES NOT** provide a tax return with the status of 02 or 03, see IRM 25.23.4.17, *Determining Tax Liability/Form 2209 Instructions*.

Note: Use CC FRM49 with a block indicator of "BB" to generate block series 74 for **all** TC 594 and 599 transactions.

If	And	Then
1. Taxable return (return shows a tax liability before prepaid credits)	1. The Master File Status is '02'	1. Input a TC 599 cc 094.
2. Taxable return (return shows a tax liability before prepaid credits)	2. The Master File Status is '03'	2. Input a TC 599 cc 044.
3. Non-taxable return (Return shows no tax liability before prepaid credits)	3. The Master File Status is '02'	3. Input a TC 599 cc 096

If	And	Then
4. Non-taxable return (Return shows no tax liability before prepaid credits)	4. The Master File Status is '03'	4. Input a TC 599 cc 046

Note: Refer to your functional IRM for instructions for the processing of the return or the routing of the return to Submission Processing. See IRM 5.19.2.4.1, *Manual Creation of a Return Delinquency Module on IDRS*, and Exhibit 5.19.2-4, *Resolving Issues with Manual Created RD Modules on IDRS*, for more information.

- (4) If a tax year(s) on the taxpayer's claim, or other years found through CCA, are not open modules on IDRS:
 1. Execute FRM49 per IRM 2.4.26.3(1b), *Command Code FRM49*. This will open the module on IDRS.
 2. Input TC 590 CC 020. This will prevent any subsequent erroneous TDI's from generating.

See IRM 25.23.4.17, *Determining Tax Liability/Form 2209 Instructions*, for more information.

25.23.2.6.6
(03-15-2022)

Reversing Unsupported Allegations of Identity Theft

- (1) There may be situations when it is necessary to reverse a pending identity theft claim (taxpayer allegation of identity theft).
- (2) A pending identity theft claim is an account with an unreversed TC 971 AC 522 and no subsequent TC 971 AC 50X.
- (3) The list below briefly describes the Miscellaneous Field Codes used when reversing unsupported identity theft claims (TC 971 AC 522):
 - **NOIDT:** In the course of resolving an identity theft issue, the employee assigned determines no identity theft occurred.
 - **NORPLY:** This code is used to close a suspended case when the taxpayer fails to provide the requested claim and/or additional information within the time specified by the employee assigned.
 - **TPRQ:** The taxpayer requests the 971 be reversed and has provided a reasonable basis for that request.
 - **IRSERR:** The 971 input was due to a typographical mistake or another internal mistake or IRS determined possible identity theft (IRSID) and later determined no identity theft occurred.
 - **IRSADM:** The 971 is causing a negative impact on another internal process or system and must be reversed to discontinue the negative impact. For example, a programming glitch prevents returns from processing.
 - **FALSE:** Reserved - TBD
 - **OTHER:** The reason for the 971 reversal does not meet any of the above reason descriptions.

25.23.2.6.6.1
(05-08-2023)

No Reply – TC 972 AC 522 NORPLY

- (1) When taxpayers do not respond to a request for more information (NORPLY) consider their claim invalid.
- (2) If the taxpayer does not respond to the request for additional documents or information and there is not enough information in the taxpayer's previously submitted correspondence to allow a referral to IDTVA take the following actions:
 1. Use Command Code REQ77 initiated from ENMOD to input a TC 972 AC 522 reflecting a Tax Administration Source Code of NORPLY and the tax year of the identity theft incident. See Exhibit 25.23.2-11, *IMF Only TC 972 AC 522 – Reversal of TC 971 AC 522*, for additional information.

Exception: If, at the time of case closure you find the Entity module has not been flagged with a TC 971 AC 522 IRSID/UNWORK, you must enter a TC 971 AC 522 UNWORK so it can be reversed with a TC 972 AC 522 NORPLY.

Reminder: The TC 972 must be post-delayed one week to allow the TC 971 to post.
 2. Follow functional guidelines for additional processing instructions. **IDTVA Employees:** See IRM 25.23.4.10.16, *No Reply*, for more procedural information.
- (3) The following is an example of a case determined to be a no reply (NORPLY):

Example: On February 14, 2017, the taxpayer contacted SBSE Exam regarding a 2015 statutory notice of deficiency. The taxpayer claimed that he MUST be a victim of identity theft as someone else claimed his dependents. The exam employee input a TC 971 AC 522 PNDCLM to flag the account as potential identity theft and requested the taxpayer provide a valid claim and/or additional information within the next 30 days. The case was put into suspense for 45 days. The taxpayer did not respond. On April 18, 2017, the exam employee reversed the pending identity theft claim using TC 972 AC 522 NORPLY and continued to work the case using normal exam procedures.

Reminder: If the taxpayer does not provide a valid claim and/or additional information when requested, proceed with case resolution assuming the taxpayer is not an identity theft victim.

Caution: If the year in question being reversed is older than the current calendar year minus 7 years, CC REQ77 will not accept the year. See IRM 25.23.2.3.8.1, *Command Code REQ77 Secondary Date and Old Case Year Issue* for more information.

25.23.2.6.6.2
(12-06-2022)

No Identity Theft (NOIDT) Determinations – TC 972 AC 522 NOIDT

- (1) When the information taxpayers submit does not substantiate their claim of identity theft, consider their claim NOIDT.
- (2) Claims of identity theft that must be marked as NOIDT include:
 - Claims of dependent related identity theft where the dependent is being claimed by the other parent.

- Claims of identity theft when a return is rejected for electronic filing due to any reason other than someone filing using an SSN as primary, secondary or dependent on a previous tax return for the same tax year.
- Claims of identity theft where the case is determined to be a mixed entity or the taxpayer's SSN is scrambled.

Note: this list is not all inclusive.

- (3) Do not reverse a TC 971 AC 522 with a NOIDT for any of the following reasons:
- Account was IRS identified (ie., CP 36 Transcripts, AC 522 with IRSID for the tax year). See IRM 25.23.4.10.15(3), *No Identity Theft (NOIDT) Determinations*.
 - The taxpayer is a victim of non-tax-related identity theft. Refer to IRM 25.23.3.2.3, *Self-Identified- Non Tax Related Identity Theft- IDT4 Overview*, for actions to take on the account.

##

#

25.23.2.6.7
(10-01-2022)
TC 971 AC 522
PNDCLM/UNWORK/IRSID
- Incorrect Tax Year

(1) If you determine an account has been marked with a TC 971 AC 522 PNDCLM, UNWORK or IRSID for an incorrect tax year:

IF	AND	Then
1) The taxpayer is reporting identity theft in TY 2012 but ENMOD reflects a TC 971 AC 522 PNDCLM, UNWORK or IRSID for TY 2013	1) And there was no identity theft in 2013	1) <ul style="list-style-type: none">Confirm there was no identity theft incident in TY 2013Reverse the TY 2013 AC 522 using TC 972 AC 522 IRSERRInput TC 971 AC 522 IRSID, PNDCLM or UNWORK, as applicable for the correct tax year (if none already exists)

IF	AND	Then
2) The taxpayer is reporting identity theft in TY 2012 but ENMOD reflects a TC 971 AC 522 PNDCLM for TY 2013	2) And there was ID theft in both tax years	2) <ul style="list-style-type: none"> Input a TC 971 AC 522 UNWORK for TY 2012.
3) There is a posted TC 971 AC 522 PNDCLM, UNWORK or IRSID for TY 2011 and a history for TY 2012 (H,PNDCLM2012)	3) And you determine no identity theft occurred in either tax year	3) Reverse the TY 2011 indicator using TC 972 AC 522 NOIDT, to reverse an UNWORK and TC972 AC 522 IRSERR to reverse an IRSID. Leave the following history H, NOIDT2012 or H, IRSERR2012 .
4) There is a posted TC 971 AC 522 PNDCLM, UNWORK or IRSID	4) And the taxpayer did not respond to your request for a claim or additional information.	4) Reverse the indicator using TC 972 AC 522 Refer to IRM 25.23.2.6.6.1, <i>No Reply – TC 972 AC 522 NORPLY</i> . Reminder: Update existing history items, if applicable.

25.23.2.7
(10-01-2018)
IMF Identity Theft Worked by Functions Outside Accounts Management IDTVA

- (1) The re-engineering effort brought accounts management and certain compliance functions under the Accounts Management Identity Theft Victim Assistance Organization. There are pockets of employees outside the new organization who will be working ID theft related issues identified using systemic applications and other applications and methods.

25.23.2.7.1
(10-01-2018)
Identity Theft Identified by Criminal Investigation

- (1) TC 971 AC 506 is applied to a taxpayer's account when Criminal Investigation (CI) identifies identity theft incidents that have tax administration effect. Such incidents can occur when a taxpayer's identity is stolen via phishing or refund schemes verified by CI.
- (2) CI refers cases to Return Integrity and Compliance Service (RICS) Return Integrity & Verification Operations (RIVO) to input TC 971 AC 506 on an account regardless of the existence of any other identity theft indicator code (AC 501, 504, or 505) that may be present on the account. Refer to Exhibit

25.23 Identity Protection and Victim Assistance

25.23.2-8, *IMF Only TC 971 AC 506- IRS Determined tax-related Identity Theft Case Closure*, and Exhibit 25.23.2-9, *IMF Only TC 972 AC 506 tax-related, Reversal of Identity Theft Case Closure, IRS Identified*, for more information about this identity theft indicator.

25.23.2.7.2
(10-01-2018)

Return Integrity and Compliance Services (RICS). Identity Theft Identified by: Return Integrity & Verification Operations (RIVO) and the Taxpayer Protection Program (TPP) Excludes Former WI Compliance Exam Operations

- (1) RIVO handles identity theft account work processes and conducts research to verify the validity of tax return information. Specifically, RIVO inputs a TC 971 AC 506 identity theft indicator on a taxpayer's account when a false tax return has been identified by the IRS, and the tax return was not filed by the valid taxpayer. See IRM 25.25.6.3, *Taxpayer Protection Program (TPP) Basic Authentication and Research*, and IRM 25.25.6.4, *Taxpayer Protection Program (TPP) High Risk Authentication (HRA) Procedures*, for additional procedures.
- (2) The **Taxpayer Protection Program (TPP)** is responsible for handling potential Identity Theft cases that are scored by a set of identity theft models in the Dependent Database (DDb) or selected through a query in Electronic Fraud Detection System (EFDS). Refer to IRM 25.25.6.5, *Responding to the Taxpayer and Case Resolution for the Taxpayer Protection Program (TPP) Telephone Assistors and Taxpayer Assistance Center (TAC) Assistors*, for additional information.

25.23.2.7.2.1
(06-17-2024)

Returns Selected by Identity Theft Filters - Taxpayers Visiting the TAC

- (1) The Taxpayer Protection Program (TPP) is responsible for handling potential Identity Theft cases. Returns are scored using a defined set of identity models in DDB; selected through filters in the Return Review Program (RRP) system; or manually selected by Return Integrity Verification Operations (RIVO). Once a return is identified as "potential" identity theft, the return is prevented from posting and either a Letter 4883C or Letter 5071C is sent to the taxpayer for verification. For additional information, refer to IRM 25.25.6, *Taxpayer Protection Program* and IRM 25.25.6.3.1, *Taxpayer Protection Program (TPP) Procedures for Power of Attorney or Third-Party Callers*.
- (2) Taxpayers who visit a TAC after receiving a TPP letter or who meet any of the other criteria in IRM 21.3.4.28.1(3), *Tax Return Related Identity Theft Issues*, will be required to authenticate their identity. A Form 14039 is **NOT** required.

Reminder: In addition to authenticating their identity, the taxpayer, if they filed the return, also must provide information off their tax return to verify they filed it. The taxpayer should bring a copy of the return so they can verify they filed the return to avoid having to reschedule their appointment. For more information, refer to IRM 25.25.6.6.6, **Referring the Caller to the Taxpayer Assistance Center (TAC) - Non-Taxpayer Protection Program Assistors** and IRM 21.3.4.2.4.5.5, *Taxpayer Issues Requiring a TAC Visit*.

(3) Authentication of Identity

- All government issued photo IDs must be the original document, photocopies are not acceptable.
- If a taxpayer indicates they have changed their name, but have **NOT** updated their records with SSA, proof of name change must be provided (e.g., marriage certificate, court documentation, etc.)
- Powers of Attorney (POAs) cannot authenticate on behalf of taxpayers who have received the Letter 5747C. If a Letter 5747C (or the account has a TC 971 AC 123 with the literal TACAUTIONLY on TXMOD), then

the taxpayer must be present at the TAC to authenticate their identity. POAs can authenticate on behalf of their clients if their client received one of the other TPP letters.

- If the taxpayer provides foreign documentation for picture identification, follow IRM 3.21.263.6.3.4.2, *Reviewing Supporting Identification Documents* to determine if it is acceptable.

Reminder: Any reference to “Taxpayer” means any person filing a return as the Primary or Secondary filer, no matter their age.

If	And	Then
<p>The Taxpayer presents a valid, current U.S. federal or state government issued form of picture identification such as:</p> <ul style="list-style-type: none"> • A driver’s license • State identification card • Passport <p>Exception: Employees must question taxpayers who state they don’t have photo identification. This will prompt the taxpayer to explain that it is due to religious beliefs. If they state it is because of their religious beliefs the exception about mailing the alternative documentation would apply. See paragraph 4 below for identification requirements for members of certain religious sects</p>		<p>Verify the taxpayer’s identity. Follow procedures in IRM 10.10.3.3.6 , Identity Proofing for Required Taxpayer Authentication. Once disclosure is completed accept the taxpayer as authenticated. . See IRM 25.25.6.5, <i>Responding to the Taxpayer and Case Resolution of the Taxpayer Protection Program (TPP) Telephone Assistors and Taxpayer Assistance Center (TAC) Assistors</i>.</p> <p>Exception: See paragraph 4 below for identification requirements for members of certain religious sects</p>

#

If	And	Then
<p>The Taxpayer presents a valid, current U.S. federal or state government issued form of picture identification such as:</p> <ul style="list-style-type: none"> • A driver's license • State identification card • Passport <p>Exception: Employees must question taxpayers who state they don't have photo identification. This will prompt the taxpayer to explain that it is due to religious beliefs. If they state it is because of their religious beliefs the exception about mailing the alternative documentation would apply. See paragraph 4 below for identification requirements for members of certain religious sects</p>		<p>If the taxpayer is an adult or minor 14, years old and above, they must provide at least one additional form of identification. If the taxpayer is a minor under the age of 14 they must provide at least 2 additional forms of identification.</p> <p>Exception: See paragraph 4 below for identification requirements for members of certain religious sects</p> <p>Note: Additional forms of identification can include current US federal or state government issued identification that is different from the first document provided:</p> <p>Reminder: Any current US federal or state government issued identification presented MUST be signed by the issuing agency and/or the taxpayer where appropriate.</p> <ul style="list-style-type: none"> • A driver's license • State identification card • Passport • Social Security Card • Tribal membership document <p>Note: A Tribal Membership card is not a federally issued ID. Currently, the Bureau of Indian Affairs is not involved with which individuals the various tribes chose to recognize as members. There is also no uniform procedure amongst the tribes to verify a member's identity. Those cards can be an additional form of ID but they are not a valid alternative to a driver's license or passport.</p> <ul style="list-style-type: none"> • Car Title • Voter Registration card <p>Note: Excludes the voter registration application</p> <p>Note: The following items are also acceptable.</p>

#

If	And	Then
		<ul style="list-style-type: none"> • Mortgage Statement • Lease agreement for rental domicile • Utility Bill with current address • Birth Certificate <ul style="list-style-type: none"> • Required: <ul style="list-style-type: none"> a. Name at Birth b. Date of Birth c. City of Birth <p>Note: Issuing city is acceptable for "City of Birth"</p> • Optional <ul style="list-style-type: none"> a. Country of birth • School Records (Under the age of 14 and/or Students Only up to the age 24) <p>Exception: Minors under 14 years of age may not have documentation with a photograph.</p> <p>Note: Students age 14-24 must still meet the photo criteria for supporting documentation.</p> <p>Note: A combination of these documents for an adult must include at least one photo ID.</p> <p>Note: IRS no longer accepts Puerto Rican birth certificates issued before July 1, 2010, due to new laws by the Government of Puerto Rico. Taxpayers with Birth certificates issued before this date must get new documentation from the Puerto Rico Vital Statistics Record Office.</p>

- (4) Members of certain religious sects (such as Amish, Mennonite and others) do not have photo IDs. In many cases a trip to the TAC presents a significant hardship to this group of taxpayers. Please advise them that if they are unable to visit a TAC, they can send the necessary document by mail to the address on the letter they received. Acceptable documents for these taxpayers are a minimum of two of the options listed below:

- Birth Certificate
- Bank Statements
- 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)

Reminder: Document (on Letterhead) from Health Care Provider (Doctor, Nurse or clinic) must have the following information verifying identity of Taxpayer:

- 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)

- (5) If taxpayer has already come to the TAC and they do not authenticate 2 or more times, the TAC will provide the "Taxpayer Cannot Authenticate" Letter 5216. Refer to IRM 25.25.6.3.4, *The Taxpayer does not Authenticate at the Taxpayer Assistance Center*, and Exhibit 25.25.6-1, *Taxpayer Protection Program (TPP) Repeater Letter 5216 - Taxpayer Cannot Authenticate*, for additional information.

Note: Refer to the following IRMs for additional guidance IRM 3.21.263.6.3.4.2, *Reviewing Supporting Identification Documents*, and Exhibit 3.21.263-8, *General Procedures for Detecting Questionable Documents*.

25.23.2.7.2.2
(10-01-2018)

MFT 32 - Overview

- (1) Beginning with 2013 returns, RICS established an MFT 32 procedure to "house" fraudulent identity theft returns discovered by the IRS. This allows certain identity theft returns to post to MFT 32 instead of posting as a TC 150 or a TC 976 on the MFT 30 account.
- (2) MFT 32 will contain tax returns that are known instances of Identity Theft (IDT). A return can be moved/posted to MFT 32 with one of the following actions:
- Posting a TC 971 AC 111 to MFT 30
 - Editing Special Processing Code (SPC) "T" on the return
- (3) When a TC 971 AC 111 posts to MFT 30 it will contain the DLN of the Identity Theft return in the MISC field of the transaction. A TC 976 with the same DLN of the Identity Theft return will post on MFT 32. When SPC "T" is edited on the return, a TC 971 AC 111 will not appear on MFT 30. For additional information regarding MFT 32 accounts, refer to IRM 25.25.6.7, *MFT 32 Procedures - How to Move Identity Theft Returns to MFT 32 During Cycles 1 - 46 and Cycles 47 - 52* in addition to your functional IRM.

Note: If a return cannot be located on MFT 30, research CC IMFOLI to determine if a MFT 32 module is present. If present, review MFT 32 for the posting of a TC 976 containing the DLN of the return in question. Research CC TRDBV to obtain the return data.

- (4) All functions will work their own MFT 32 cases moved in error. For more information, see IRM 25.25.6.7.1, *Taxpayer Protection Program (TPP) Assistors, Taxpayer Assistance Center (TAC) Assistors, and Identity Theft Victims Assistance (IDTVA) Assistors MFT 32 Reversal Criteria & Procedures*.

25.23.2.7.3
(09-06-2023)
Identity Theft Identified by Submission Processing

- (1) Submission Processing reviews returns that unpost because the taxpayer did not provide an IP PIN that matches the IP PIN listed on the account. If the review determines that the return was not filed by the SSN owner, SP will move the return to MFT 32 and input a TC 971 AC 506 identity theft indicator on the account.
- (2) Additional guidance for procedures used by Submission Processing can be found in the following IRMs:
 - IRM 3.28.4.4.6, *Inputting Identity Theft Indicators*.
 - IRM 3.12.179.46, *UPC 147 Reason Code 0 Identity Protection PIN (IP PIN)*.
 - IRM 3.28.4.4, *Unpostable Code (UPC) 147 Reason Code (RC) 0*.
 - *Document 6209, Section 8B-3, Unpostable Codes - IMF*.
- (3) See Exhibit 25.23.2-8, *IMF Only TC 971 AC 506 — IRS Determined Tax-Related Identity Theft Case Closure*, for more information about this identity theft indicator.
- (4) SP will edit paper tax returns containing a Form 14039 with a Special Processing Code (SPC) 8. The SPC 8 systemically generates a TC 971 AC 522 indicating receipt of an identity theft claim. CP 01S is systemically issued to the taxpayer confirming receipt of the Form 14039. Refer to Exhibit 3.21.3-1, *Attachment Guide*, for additional information.

25.23.2.8
(10-01-2024)
Miscellaneous Identity Theft Indicators

- (1) The Service developed additional indicators to capture specific identity theft issues with specific characteristics. The indicators include:
 - **AC 504:** Both non-tax-related and specific tax-related identity theft issues
 - **AC 505:** IRS loss of PII
 - **AC 523:** Reserved
 - **AC 524:** Locking Decedent Accounts
 - **AC 525:** Employment related identity theft
 - **AC 527:** Online Access blocked
 - **AC 528:** IP PIN Enrollment/Suppression Bypass
 - **AC 545:** Reserved for IPSO use **ONLY**.

Reminder: Identity Theft indicators AC 501, AC 504, AC 505, AC 506, AC 522, AC 523, AC 524 and AC 525 never expire.

25.23.2.8.1
(09-06-2023)
IMF TC 971 AC 504

- (1) TC 971 AC 504 is intended for use on non-tax-related identity theft allegations only. For additional information see IRM 25.23.2.8.1.2, *TC 971 AC 504 - Miscellaneous Field Code SPCL1, SPCL2, RPM1, RPM2, RPM3, RPM4, and EAFAIL* and IRM 25.23.3.2.3, *Self-Identified - Non-Tax-Related Identity Theft – IDT4 Overview*.

Reminder: If a TC 971 AC 504 is input as a closing code, then a reversal of the existing TC 971 AC 522 is not required.

- (2) IDTVA will continue to use TC 971 AC 504 with Miscellaneous Field Codes ACCT, ACCT-M, EMPL, EMPL-M, ICMCCA, NKI or NKI-M for taxpayer allegations of identity theft that do not affect tax administration. For additional

25.23 Identity Protection and Victim Assistance

information, IRM 25.23.2.8.1.1, *TC 971 AC 504 with Miscellaneous Field Codes ACCT, ACCT-M, BOTH, BOTH-M, EMPL, EMPL-M, NKI or NKI-M.*

- (3) Other BOD/Functions will use TC 971 AC 504 with Miscellaneous Field Codes SPCL1, SPCL2, RPM1, RPM2, RPM3, RPM4, and EAFail to mark taxpayer accounts when certain conditions apply. For additional information, see IRM 25.23.2.8.1.2, *TC 971 AC 504 - Miscellaneous Field Code SPCL1, SPCL2, RPM1, RPM2, RPM3, RPM4, and EAFail.*

Note: Do not disclose to the taxpayer the TC 971 AC 504 with Miscellaneous Field Codes SPCL1, SPCL2, RPM1, RPM2, RPM3, RPM4, and EAFail.

25.23.2.8.1.1

(02-02-2024)

TC 971 AC 504 with Miscellaneous Field Codes ACCT, ACCT-M, BOTH, BOTH-M, EMPL, EMPL-M, ICMCCA, NKI or NKI-M

- (1) Input of TC 971 AC 504 requires a miscellaneous (MISC) code when input. AC 504 with Miscellaneous Field Codes ACCT, ACCT-M, EMPL, EMPL-M, ICMCCA, NKI or NKI-M are used for non-tax- related incidents and are reserved for use by IDTVA employees.

Reminder: A TC 971 AC 504 with the Miscellaneous Field Codes above are used as closing codes. Reversal of an existing TC 971 AC 522 is not required.

Example: Events such as a home robbery, PII was used for unemployment claims, data breach or lost/stolen PII that compromises or involves the taxpayer's SSN, putting the taxpayer at risk for tax related identity theft in the future.

Caution: Command Code REQ77 will not accept a tax year that is seven years prior to the current date. See IRM 25.23.2.3.8.1, *Command Code REQ77 Secondary Date and Old Case Year Issue* for more information.

Note: If a taxpayer subsequently claims tax-related identity theft, and the account was flagged with TC 971 AC 522 (PNDCLM, UNWORK, or IRSID) and TC 971 AC 504 (ACCT, ACCT-M, BOTH, BOTH-M, EMPL, EMPL-M, ICMCCA, NKI or NKI-M), do not request the taxpayer provide Form 14039 or police report and proof of identity if the TC 971 AC 522/504 are within the 3 year period.

- (2) Non-tax related incidents are usually identified when the taxpayer/IDT victim checks box "2" in Section B of the Form 14039. The following MISC codes are used when resolving/closing a Non-Tax-related incident:

MISC Code	Definition
ACCT	Reserved
ACCT-M	Reserved
BOTH	Reserved
BOTH-M	Reserved
EMPL	Victim's SSN used for employment and/or unemployment insurance.

MISC Code	Definition
EMPL-M	Same as above – “M” identifies cases requiring a manual 4402C/SP letter instead of a systemic notice (CP 01C and CP 701C)
ICMCCA	Used to indicate impacted tax years identified through Complete Case Analysis (CCA) Note: There is no manual letter version for this MISC Code. A manual letter will be indicated by the literal on the year identified by the taxpayer.
NKI	No Known Impact was identified
NKI-M	Same as above – “M” identifies cases requiring a manual 4402C/SP letter instead of a systemic notice (CP 01C and CP 701C)

- (3) One TC 971 AC 504 per ACCOUNT (TIN) is sufficient when there is no impact to tax administration for **any** tax year. If there are multiple years and tax administration is not impacted for any year, input the TC 971 AC 504 on the earliest year.

Example: Form 14039 is filed reporting the taxpayer’s wallet and Social Security Card were stolen in 2020. Research of the account shows there are no tax related issues. TC 971 AC 504 with MISC “NKI” will be input for tax year 2020.

- (4) TC 971 AC 504 will be input for each tax year the taxpayer has been determined to be a victim of income related IDT not affecting tax administration.

Example: Form 14039 is filed reporting someone is working under the taxpayer’s Social Security Number (SSN) for tax year 2021. You confirm the identity theft for tax year 2021. Through CCA you determine the taxpayer is also a victim of income related identity theft that does not affect tax administration for tax years 2019 and 2020. TC 971 AC 504 with MISC “EMPL-M” will be input for tax year 2021. TC 971 AC 504 with MISC **ICMCCA** will be input for tax years 2019 and 2020.

- (5) When inputting TC 971 AC 504, determine the secondary date using the following table:

If	Secondary Date
1) Income Related IDT	The tax year impacted in the format of 1231YYYY. Example: TY 2021 is impacted. The secondary date used will be 12312021.
2) All other non-tax-related	The incident date in the format of MMDDYYYY. Refer to Exhibit 25.23.2-4, <i>IMF Only TC 971 AC 504</i> , for additional information. Example: The taxpayer is part of a data breach at their place of employment on 05172021. The secondary date used will be 05172021.

- (6) If IRS employees are contacted by a taxpayer indicating a non-tax-related identity theft, see IRM 25.23.12.2, *Identity Theft Telephone General Guidance*, and IRM 25.23.3.2, *Identity Theft - Paper Overview*.

Exception: Taxpayer Assistance Center employees must refer to their IRM 21.3.4.28.4, *Non-Tax Related Identity Theft Issues*, for procedures on how to assist taxpayers who walk into a Field Assistance Office.

25.23.2.8.1.2
(09-06-2023)

**TC 971 AC 504 -
Miscellaneous Field
Code SPCL1, SPCL2,
RPM1, RPM2, RPM3,
RPM4, and EAFail**

- (1) In 2014, IPSO expanded the use of TC 971 AC 504. to flag taxpayer accounts for the conditions listed in the table below.

Reminder: TC 971 AC 504 with Miscellaneous Field Codes SPCL1, SPCL2, RPM1, RPM2, RPM3, RPM4, and EAFail may be tax-related. If a TC 971 AC 504 is input as a closing code then a reversal of an existing TC 971 AC 522 is not required.

Note: Do not disclose to the taxpayer the TC 971 AC 504 with Miscellaneous Field Codes SPCL1, SPCL2, RPM1, RPM2, RPM3, RPM4, and EAFail.

- (2) When entering a TC 971 AC 504 with a Miscellaneous Field Codes SPCL1, SPCL2, RPM1, RPM2, RPM3, RPM4, and EAFail, the Secondary Date field will reflect the related tax year. The Secondary Date field on CC REQ77 is limited to the current calendar year (cannot be the current day or any future date) and 7 prior years. See IRM 25.23.2.3.8.1, *Command Code REQ77 Secondary Date and Old Case Year Issue* for more information. It is recommended the REQ77 IAT tool be used when entering this indicator and MISC code.

- (3) This table describes when these MISC codes will be used with a TC 971 AC 504:

MISC Code	Definition
SPCL1	Will be used to mark an account when there is at least one incident of failed High-Risk Disclosure during a phone call and a taxpayer is requesting their Adjusted Gross Income (AGI) or Self Select PIN (SSP) so that they can e-file their tax return. These taxpayers will not be issued an IP-PIN based upon the input of AC 504 SPCL1. However, an IP-PIN may have been issued based upon the input of another identity theft code.
SPCL2	Will be applied to a taxpayer's account when the taxpayer makes a phone inquiry or submits a Form 14039 under their SSN claiming they are a victim of BMF ID theft that is affecting their SSN.
RPM1, RPM2, RPM3, RPM4	Used by IDTVA to flag closed and resolved Return Preparer Misconduct cases effective January 1, 2014.
EAFAIL	Formerly used by RICS to flag accounts where the Electronic Filing PIN (EFP) Application was linked to a telephone line that had been blocked after a series of attempts to secure a PIN. These taxpayers were not issued an IP-PIN based upon the input of AC 504 EAFAIL. The Electronic Filing PIN (EFP) Application is no longer functional. However, an IP-PIN may have been issued based upon the input of another identity theft code.

Example: The taxpayer receives IRS notices related to a business for which the taxpayer has no affiliations. The taxpayer asserts he/she has never applied for an EIN and has never owned or operated a business. The employee will apply TC 971 AC 504 with Miscellaneous Field Code SPCL2 using command code REQ77.

Reminder: Prior to January 1, 2014, SPCL2 was used by the Accounts Management and Compliance to flag closed and resolved Return Preparer Misconduct cases. These taxpayers were not issued an IP PIN based upon the input of AC 504 SPCL2. However, an IP PIN may have been issued based upon the input of another identity theft code.

- (4) If, after careful review and analysis of the BMF accounts, the employee working the identity theft issue determines no identity theft occurred, the employee will reverse the TC 971 AC 504 SPCL2 on the taxpayer's SSN. Refer to Exhibit 25.23.2-5, *IMF Only TC 972 AC 504 — Reversal of TC 971 AC 504*, for additional information.
- (5) The presence of AC 504 SPCL1, SPCL2, EAFail, or RPM1, RPM2, RPM3, RPM4 should not prevent the taxpayer from receiving an IP PIN if they have lost, misplaced or not received their IP PIN. Refer to IRM 25.23.2.9.4, *Lost, Misplaced or Non-Receipt of IP PIN Overview*, IRM 21.1.3.2.3, *Required Taxpayer Authentication* and IRM 21.1.3.2.4, *Additional Taxpayer Authentication*, for additional information.

25.23.2.8.1.3
(05-03-2018)

**IMF Only - Manually
Reversing TC 971 AC
504**

- (1) In some instances, it may be necessary to manually reverse TC 971 AC 504. If reversal is indicated (TC 972 AC 504), see Exhibit 25.23.2-5, *IMF Only TC 972 AC 504 - Reversal of TC 971 AC 504*, for a description of reasons for the reversal.
- (2) **Taxpayer requests:** In situations where the taxpayer is requesting you reverse the TC 971 AC 504, the taxpayer **MUST pass high risk disclosure** prior to your making any account adjustments. Refer to IRM 21.1.3.2.3, *Required Taxpayer Authentication*, and IRM 21.1.3.2.4, *Additional Taxpayer Authentication*, for additional information.
- (3) The taxpayer must provide a reasonable explanation as to why the TC 971 AC 504 marker should be removed.

Example: The taxpayer states identity theft did not occur. The taxpayer thought a package containing PII was stolen, but the package was returned to the taxpayer in its original sealed condition.

Note: Reversals of the AC 504 with any of the Miscellaneous codes in the table below is not limited to IDTVA-I and can be done by any employee once the request has been validated.

If	AND	THEN
The taxpayer passes high risk disclosure	The Miscellaneous Field on the TC 971 AC 504 contains any of the following: <ul style="list-style-type: none"> • ACCT • ACCT-M • BOTH • BOTH-M • EMPL • EMPL-M • NKI • NKI-M 	Reverse the TC 971 AC 504 as directed in Exhibit 25.23.2-5, <i>IMF Only TC 972 AC 504 - Reversal of TC 971 AC 504</i> , using “ TPRQ ” in the Miscellaneous field

- (4) If you determine the TC 971 AC 504 should be reversed for other than a taxpayer request, refer to the table in Exhibit 25.23.2-5, *IMF Only TC 972 AC 504 — Reversal of TC 971 AC 504*, for a list of valid Miscellaneous Field Codes.

#

25.23 Identity Protection and Victim Assistance

[illegible][illegible]

#

25.23.2.8.2
(03-16-2023)
**IRS Data Breaches- TC
971 AC 505**

- (1) Input of TC 971 AC 505 is limited and reserved for use by Privacy, Governmental Liaison, and Disclosure (PGLD) Incident Management employees. However, this indicator will be visible and available for reference on the individual's account. See Exhibit 25.23.2-6, *IMF Only TC 971 AC 505 — IRS Data Breaches*, and Exhibit 25.23.2-7, *IMF Only TC 972 AC 505 — Reversal of TC 971 AC 505*, for more information about this indicator.

Note: When a TC 971 AC 505 is input on an account, PGLD does **not** ask for or require identity theft claims or additional information, as identity theft may not have occurred as of the date of the input of this action code.

- (2) TC 971 AC 505 is applied to a taxpayer's account when all of the following occur:
- A taxpayer's PII was lost, breached, disclosed, or stolen.
 - The breach risk assessment results in a high risk of harm to the potentially impacted taxpayer.
 - The IRS notifies the taxpayer of this data breach.

Example: Taxpayer case files containing PII were lost while being shipped from one location to another. Since the breach risk assessment resulted in a high risk of harm, the Incident Management Program will send notification letters to the potentially impacted taxpayers.

- (3) The TC971 AC505 does not block, or prevent, online system access, will not stop registration for online services, including Get Transcript or IP PIN and will not stop paper requests for a transcript (Form 4506/T). Blocking accounts from on-line access is a separate action. If an account is blocked from on-line access, you will see an TC 971 AC 527 on the entity module. Accounts previously disabled from the Secure Access application due to an incident or breach prior to May 2016, such as the Get Transcript Incident, have been opened and the taxpayer can now access the application. Accounts that remain disabled in Secure Access can be identified by an unreversed TC 971 AC 527 WI BREACH DSABLD on the entity. If there is an unreversed AC 527 on the account, See IRM 25.23.2.8.6, *Disabled Accounts TC 971 AC 527*.
- (4) The taxpayer will receive a data breach notification Letter 4281C, (IM Breach Notification Letter), from the IRS advising him/her that information controlled by the IRS may have been disclosed to unauthorized individuals. The notification letter contains information related to identity protection and an identity protection service arranged for the taxpayer by the IRS. Refer to IRM 25.23.12.4.8, *Responses to IM Breach Notification Letter 4281C*, for additional information.

Note: The taxpayer must call the company identified in the letter to enroll in the free identity protection service.

- (5) PGLD inputs TC 971 AC 505 on an account even when another identity theft indicator code (AC 501, 504, or 506) is present on the account. In some instances, it may be necessary for PGLD personnel to manually reverse the TC 971 AC 505 with a TC 972 AC 505.
- (6) The AC 505 is used to track data breaches. For information on the Incident Management Program see IRM 10.5.4.5.1.1, *Applying the IRS Data Breach Tracking Indicator to IRS Data Breaches*.

25.23.2.8.3
(09-15-2017)

(1) RESERVED

#

- 25.23.2.8.4
(02-02-2024)
**Locking Decedent
Accounts - TC 971 AC
524**
- (1) The TC 971 AC 524 is an identity theft indicator used to lock the account of deceased taxpayers. It prevents a deceased taxpayer's TIN (SSN or ITIN) from being used as the primary, secondary or dependent TIN on a current or subsequent year federal income tax return. Account locks can be applied both manually and systemically using internal or external information. However, input of the TC 971 AC 524 is limited and reserved for use by IPSO and RICS Taxpayer Protection Program (RICS TPP).

(2) TC 971 AC 524 can be viewed on the taxpayer's entity using command codes ENMOD or IMFOLE.

(3) The identification, development, and implementation of specific population categories for the TC 971 AC 524 will be phased in by IPSO with the goal of creating a comprehensive list of taxpayers who do not have a filing requirement. Account locks may be initiated either manually or systemically.
Manually: A manual lock is placed on a deceased taxpayer's account when a date of death (DOD) is present on the tax module and the account is identified by CI or Return Integrity & Verification Operations (RIVO) as fraudulent.
Systemically: A systemic lock is placed on a deceased taxpayer's account when we process a final return with a DOD.

(4) Systemic Locking of Deceased Taxpayer accounts occurs when all of the following are true:
 - A date of death is present on the tax module; and
 - A personal representative has filed a final return; and
 - Computer Condition Code A, F or 9 is placed on the account as indicated in the table below:
- | A final return is filed with CCC: | Then a TC 971 AC 524 is applied to |
|-----------------------------------|------------------------------------|
| F | The primary taxpayer |
| 9 | The secondary taxpayer only |
| A | Both Taxpayers |
- Note:** Refer to IRM 3.11.3.10.5, *Computer Condition Codes for Decedent Returns*, and IRM 3.13.5.138, *Computer Condition Codes (CCCs)*, for additional information.

(5) Manual Locking occurs when individual accounts are identified by a business function and provided to IPSO or RICS for input using a systemic tool.

(6) Returns filed on decedent accounts containing an unreversed TC 971 AC 524 DECD, will be prevented from processing.
- Electronically Filed Returns
- 25.23.2.8.3

Internal Revenue Manual

Cat. No. 67662Y (08-26-2024)
Any line marked with a #
is for **Official Use Only**

If the taxpayer is	And the source code is	Then
Primary	DECD	Taxpayer will receive a reject code IND 901
Secondary	DECD	Taxpayer will receive a reject code IND 941

Paper Filed Returns

If the taxpayer is	And the source code is	Then
Primary or Secondary	DECD	<ol style="list-style-type: none"> 1. Return will unpost as UPC 147 RC 4 2. Return will be auto-archived 3. CP 01H, We are Unable to Process Your Return, is mailed to the taxpayer <p>Note: For information on CP 01H, refer to IRM 21.6.6.2.21.3, CP 01H Notice or Letter 12C Decedent Account Responses.</p>

(7) UPC 147 Reason Code 4 will only be set if one of the two conditions below are present:

- An unreversed TC 971 AC 524 is present on the Entity Module. Any return attempting to post that has a tax period after the Secondary date of the TC 971 AC 524 will unpost and be auto archived. There are no exceptions.
- No TC 971 AC 524 is on the Entity Module but during return processing Special Processing Code (SPC) 9 was entered on the return (see ERS EC 028). Entering SPC 9 on a return will unpost the return as UPC 147 RC 4 and the return will be auto-archived. It will unpost ONLY the return that SPC 9 was input on. This leaves the module open for posting of a legitimate return. Do NOT refer the account to ECU to unlock (the account is not locked). If it is believed that the unposted return is the legitimate return it must be requested from Files using CC ESTAB and reprocessed.

25.23.2.8.4.1
(11-01-2021)

**Manually Reversing TC
971 AC 524 - Date of
Death Present on
Command Code INOLES**

- (1) Input of a TC 972 AC 524 will reverse a TC 971 AC 524 and will “unlock” the account. If there is a date of death on CC INOLES, the input of the TC 972 AC 524 is limited and reserved for:
 - Identity Protection Strategy & Oversight (IPSO)
 - RICS Taxpayer Protection Unit (RICS TPP)
 - Submission Processing Entity Control Unit (ECU)
- (2) To unlock a decedent account, a taxpayer must provide information to support their request.
- (3) If a taxpayer contacts IRS relating to a locked account and there is a Date of Death (DOD) on the account and an unreversed TC 971 AC 524 DECD is present, ALL of the following documentation MUST be provided by the taxpayer:
 - a. Original/Copy of Letter/Notice from the Social Security Administration that communicates that the taxpayer is not deceased
 - b. A photocopy of at least one of the following:
 - Passport or Driver’s License
 - Social Security Card
 - Other valid US Federal or State Government issued identification;
 - c) A copy of their tax return with an original signature(s);

Exception: If the request is not related to a rejected return but is being made solely to perfect the date of death, the taxpayer does not need to provide a copy of a tax return. Instruct the taxpayer to contact the Social Security Administration (SSA) to correct the erroneous Date of Death (DOD).

Instruct the taxpayer to send all of the above information to the same service center the taxpayer used to file his or her original tax return.

Note: Prepare Form 4442 and forward the documents provided by the taxpayer to the ECU.

- (4) If a taxpayer contacts IRS relating to a locked account and there is no longer a Date of Death (DOD) on the account and an unreversed TC 971 AC 524 DECD is present on the entity, refer to Exhibit 25.23.2-14, *TC 971 AC 524- Locking SSNs - Applies to IMF Accounts Only*, Exhibit 25.23.2-15, *TC 972 AC 524- Reversal of TC 971 AC 524*, and IRM 3.12.179.46.2, *UPC 147 Reason Code 4 No Filing Requirement*, for information.

25.23.2.8.4.2
(02-02-2024)

**Manually Reversing TC
971 AC 524 - No Date of
Death Present on
Command Code INOLES**

- (1) In situations where there is no DOD on INOLES CSRs may, after completing the required taxpayer authentication, reverse TC 971 AC 524.

Caution: If there is a date of death on INOLES, do NOT reverse the TC 971 AC 524. Refer to IRM 25.23.2.8.4.1, *Manually Reversing TC 971 AC 524 - Date of Death Present on Command Code INOLES*, for procedures. If Death Date field on Command Code IMFOLE has a date other than all zeros, then one or more tax modules contains a TC 540 which needs to be reversed. Please see IRM 21.6.6.2.21.1(4), *Updating the Entity on Decedent Accounts*.

- (2) If a taxpayer contacts IRS relating to a locked account and there is no longer a Date of Death (DOD) on the account and an unreversed TC 971 AC 524 DECD is present on the entity, reverse the TC 971 AC 524. To reverse a TC 971 AC 524, you will need to access command code REQ77:

1. Access command code REQ77 from ENMOD
2. Enter TC 972 in the TC field
3. Enter the transaction date of the TC 971 AC 524 being reversed in the TRANS-DT field
4. In the Secondary Date Field, enter the tax year from the TC 971 AC 524. If there is no tax year present, use "1231" and the year you are reversing. If the year in question is 2015, the Secondary Date field date would be input as "12312015".

Note: If you are reversing the current year, input the current date minus one day, as REQ77 will not accept future dates,

5. In the MISC Field enter the appropriate BOD, Program, and Tax Administration Source Code describing why the TC 971 AC 524 is being reversed (use IRSERR when there is no date of death present)

For additional input information, refer to Exhibit 25.23.2-15, *TC 972 AC 524-Reversal of TC 971 AC 524*.

25.23.2.8.5
(10-01-2024)
**Employment-related
Identity Theft – TC 971
AC 525**

- (1) Employment Related Identity Theft occurs when someone, other than the valid SSN owner, uses the SSN to obtain or retain employment. Employment Related Identity Theft is considered "non-tax" related because it does not involve the filing of a fraudulent income tax return. However, the income generated by the person other than the valid SSN owner may have a tax account impact if it results in the assessment of additional tax if not identified and treated prior to the assessment.

#

Note: Employment-related identity theft is not a tax administration issue; therefore, no TC 971 AC 522 is required.

#

Note: The potential misuse of the taxpayer's SSN in this manner is unrelated to and has no impact on the taxpayer's tax return or their ability to file a tax return or receive a refund.

- (3) The TC 971 AC 525 indicator code is systemically applied to the valid SSN owners account when IRS identifies an ITIN/SSN mismatch involving the taxpayer's SSN. The placement of an indicator on the account of the valid SSN

25.23 Identity Protection and Victim Assistance

owner is not exclusive to taxpayers who have earned income or indicate that the recipient has earned income. The placement of an indicator reflects the potential use of the SSN for employment by another person. The indicator will be applied a maximum of one time each year regardless of how many times the SSN was used in the same tax year. More than one indicator may be applied in the same calendar year if the ITIN/SSN mismatch was identified on multiple tax years that are processed in the same year. See the table below for specific situations and the actions or explanations for each:

Situation	Action/Explanation
SSN does not exist on Master File	A TC 971 AC 525 indicator will not post if there is no account on Masterfile. There is no need to establish an account if the identified SSN does not exist on Master File (MF) solely for the purpose of placing an AC 525 indicator.
Dependent and Minors received a notice	The CARES Act allowed for advance payment of the Recovery Rebate Credit (referred to as Economic Impact Payments (EIP)) including individuals receiving Supplemental Security Income (SSI) and SSA Disability. As a result, dependent accounts were created on Masterfile using a TC 000. The entity account displays the dependent's parent on the "CONT-OF-PRIM-NM" line. These accounts contain a TC 971 AC 199 MISC CODE: SSA 1099 DSI. A TC 971 AC 525 indicator may be placed on these accounts if a mismatch is identified.
A person does not have a filing requirement but used the Non-Filer Tool to receive an Economic Impact Payment (EIP)	If a person used the "Non-Filer" tool to register for an Economic Impact Payment. Master File created a basic 2019 Form 1040 filing, to generate the payment. A TC 971 AC 525 indicator may be placed on the account if a mismatch is identified.

Situation	Action/Explanation
Cross Referencing to Identify the Source of the Misuse	applied to the ITIN taxpayer's account and there is no cross-reference between the ITIN on the originating return and SSN on the mismatched W-2.
Misuse cause unknown	IRS is not aware if the misuse of the taxpayer's SSN is intentional or accidental due to a mistake when preparing the Form W-2. Due to the potential for harm to the taxpayer if their SSN was compromised, IRS is treating this incident as a "potential" misuse situation and providing guidance on protecting personal and financial information as a proactive protective action.
Transcript Request	If the taxpayer requests copies of any of their tax information, such as transcripts or returns, refer to procedures in IRM 21.2.3.5.8, <i>Transcripts and Identity Theft</i> , for guidance.

#

- a. Authority for systemic and manual input of the TC 971 AC 525 is limited and reserved for use by Accounts Management Identity Protection (IP) staff.
 - b. The placement of the indicator on the taxpayers account prevents any income from the Form W-2 that does not belong to the valid SSN owner from being assessed against their account. There is no other impact to the taxpayer's account.
 - c. TC 971 AC 525 can be viewed on the taxpayer's entity module using command codes ENMOD or IMFOLE.
- (4) Notifications are issued to taxpayers who had a TC 971 AC 525 indicator placed on their account after January 1, 2017. Notifications are issued via CP01E (*CP701E for Spanish*) Employment Related Identity Theft notice using the name(s) and address on the last posted return (i.e., address of record). The CP01E /CP701E is generated 2 cycles after the posting of the AC 525 indicator.

Note: Taxpayers who received an indicator prior to January 1, 2017 will be notified if an incident occurs, and an additional indicator is placed on their account after January 1, 2017

25.23 Identity Protection and Victim Assistance

Note: While a taxpayer's SSN may be impacted in subsequent years, the CP01E notice will only be issued to the same taxpayer once every 3 years.

Example: If a taxpayer receives a CP01E in 2018 and an employment related IDT incident occurs again in 2019, 2020 and 2021, an AC 525 indicator will be applied to the taxpayers account to document an identified mismatch, but the taxpayer will not receive another CP01E until 2021.

- a. TC 971 AC 804 with a MISC of 001E will post to master file when the CP01E is generated.
- b. The name(s) displayed on the notice reflect the name(s) on the taxpayer's account.

Note: If the notice contains 2 names, the impacted taxpayer will always be the first name listed on the notice.

Note: If the notice is addressed to a child, then the child's SSN may have been misused. Children may be impacted in the same way as adults and should follow the same protection guidelines.

- (5) While the CP01E/701E is an informational notice only, taxpayers may react to the notice by telephone, correspondence or visiting a TAC. When responding to taxpayer inquiries, refer to the following information:

- a. Ask the taxpayer about which notice they are calling. If the taxpayer cannot find the notice number, ask them to look on the upper right-hand corner and clearly recite the notice number. If necessary, repeat the notice number, "C, P, O, 1, E". Pronounced "See Pea Oh 1 E" or See Pea Zero 1 E".

Exception: Employees answering APP 162 and/or working with Spanish speaking taxpayers should continue to identify the caller's issue/notice in Spanish and are excepted from referencing the notice number as "C, P, O, 1, E".

Reminder: The CP01E and CP701E notices are issued systemically without regard to the recipients age, filing history or other criteria.

- b. Full disclosure and authentication is required for account related calls only. See IRM 21.1.1.4 (4), *Communication Skills*, for more information.
- c. When a taxpayer or third party contacts the IRS, and is only requesting general information regarding the CP01E, authentication and account access is not required. See IRM 21.1.1.4, *Communication Skills* for more information. Information that is contained within the CP01E or on IRS web pages is considered public information and can be provided without authentication.

Note: There is no additional information regarding the source action or W-2 document available on the taxpayers account.

- d. When a taxpayer or third-party contacts the IRS, because the first name on the notice is minor child, dependent, or other non-filer, advise the caller that Employment Related Identity theft is not related to the filing of a tax return. The notice was issued because the dependents SSN may have been used for employment. A minor child, dependent, or non-filers

personal information is just as vulnerable to identity theft. Because of the increased risk of identity theft, we are providing information protecting the impacted persons financial or credit records (if applicable).

Note: The notice contains general information that is provided to all impacted persons and is not specific to tax return filers. Some protective measures may not apply to all impacted persons. The impacted persons age or lack of financial or credit history may prevent the creation of accounts on some suggested web pages that require a review of income and credit information and the ability to obtain an IP PIN.

- e. When a taxpayer or third-party contacts the IRS, regarding a deceased person, be empathetic with the caller and advise the caller that the notice was issued to provide information on checking the decedents financial or credit records to see if there may be any impact to an estate situation.
- f. If account access is requested or necessary, the taxpayer or third party must be authenticated. See IRM 21.1.3.2.3, *Required Taxpayer Authentication*, and either IRM 21.1.3.2.4, *Additional Taxpayer Authentication*, for taxpayers or IRM 21.1.3.3, *Third Party (POA/TIA/F706) Authentication*, for third party contacts.

Note: Third party contacts must be authorized by an existing and valid Form 2848, Power of Attorney and Declaration of Representative, or Form 8821, Tax Information Authorization prior to discussing account information.

- g. Under no circumstances will assistors offer to, or attempt to research, the source of the AC 525 indicator including but not limited to, the tax return and/or Form W-2. There is no link to the source document and identification of the source of the indicator is not possible. Taxpayers will be provided general information only.
- h. In all cases, refer the taxpayers to the following resources on IRS.gov for additional information:
 - *Understanding Your CP01E Notice*,
 - *Guide to Employment-Related Identity Theft*
 - and *Taxpayer Guide to Identity Theft*
- i. In addition, advise taxpayers to take the following steps to protect their financial and tax accounts as well as their personal information:

Action	Description
If they do not currently have one, they may request an Identity Protection PIN (IP PIN) to protect their tax account.	There are now 3 options for the taxpayer to get an IP PIN. See IRM 25.23.2.9.1, <i>Participating in the IP PIN Program</i> for information on how the taxpayer can obtain, request or apply for an IP PIN.

Action	Description
Monitor their credit report and all financial accounts	Obtain a copy of all financial and credit records and review them for unusual or unauthorized activity. Obtain a copy of their credit report by contacting any one of the three nationwide credit reporting companies online or through the company's toll-free numbers listed in the CP01E Notice.
Place a fraud alert on credit accounts	As an extra precaution, contact one of the credit agencies listed on the CP01E and request that a fraud alert be placed on all credit accounts
File a complaint with the Federal Trade Commission	Contact the Federal Trade Commission at: www.IdentityTheft.gov , or call FTC's Identity Theft Hotline: 1-877-438-4338; TTY: 1-866-653-4261
Review Social Security Administration records to ensure that their earnings records are correct	Sign up for an electronic account at www.SSA.gov , to check for excessive income being reported

- (6) Letter 0544C: Due to a programming error that occurred in 2017 and 2018, some spouses who were listed as the secondary taxpayer on ITIN returns received a CP01E or CP701E when there was no identified ITIN/SSN mismatch. Beginning in May of 2019, these taxpayers will receive a 0544C letter notifying them the original CP 01E notice they received in 2017 or 2018 was issued in error; they are not victims of employment related IDT. When responding to these inquiries, apologize to the taxpayer and let them know:
- The original letter was sent to them in error
 - The identity theft indicator that was mistakenly applied to their account was removed.
 - If they have any other identity theft indicators that were applied to their account that were unrelated to this incident, they are still in place and active.
 - There is no impact to their tax account
 - They should continue to file their tax returns, and pay their tax, normally.

The letter can be found on ENMOD as ltr0544C with a literal of SP525APOLG. A TC 972 AC 525 which reversed the original TC 971 AC 525 indicator is also present on ENMOD.

- (7) **Field Assistance (TAC) Only:** If the TAC visit has unanswerable questions or needs additional assistance, complete Form 4442 "Inquiry Referral" by completing boxes 1 – 4, 8 – 10 and 13 – 14. In section B, input "CP01E TAC Center Visit" and the taxpayer's question. Either enter the taxpayer's telephone number in box 24, or the taxpayer's e-mail address in box 25, and enter the

question or issue in Section B. Forward the completed Form 4442 via encrypted email to: *TS CAS:AM:IPSO Employment Identity Theft.

Note: When forwarding Forms 4442 via encrypted e-mails, managers may wish to consolidate all forms for a specific day into a single e-mail to reduce the number of e-mails and avoid overloading the mailbox.

25.23.2.8.6
(05-08-2023)

#

- (4) The taxpayer may not have received notification of the disabled online account. Verification for on-line services is done by a 3rd party and we cannot assist in the verification process.

25.23.2.8.6.1
(03-17-2023)

#

- (2) If the taxpayer states they did not receive their CP 01A or it was lost, or they have a TC 971 AC 527 on their account and can't retrieve their IP PIN, they can have the IP PIN reissued, in most cases. See IRM 25.23.2.9.4.1 , *Lost, Misplaced or Non-Receipt of IP PIN* for procedures to reissue their IP PIN

25.23.2.8.6.1.1
(03-16-2023)

#

[illegible]

[illegible]

#

25.23.2.8.7
(10-01-2024)
TC 971 AC 528

- (1) The TC 971 AC 528 identity theft indicator is mainly used to enroll individuals into the IP PIN program, who verified their identity through Form 15227, Application for An IP PIN, or an in-person Taxpayer Assistance Center (TAC) appointment.

Exception: The TC 971 AC 528 can be used to bypass certain CP01A suppression criteria.

- (2) The table below describes the various miscellaneous codes used with the TC 971 AC 528:

Miscellaneous Field	Description	Input By
WI IPSU TPRQ	Input after Form 15227 is approved. See IRM 25.23.3.2.7	IDTVA – IDTX Trained Employees
WI FA TPRQ	Input after in-person TAC verification is approved	Headquarters
WI IP DEPND	Input after a Tax-related identity theft issue is identified for a dependent. See IRM 25.23.4.10.14	IDTVA – Full Scope Trained Employees
WI IP TPRQ	Bypass certain CP01A suppression criteria	Headquarters

##

#####

- ##

##

- ### **25.23.2.8.9.1**

25.23 Identity Protection and Victim Assistance

etc.), in the "Proposed Resolution" field, include in your recommendation the case be reassigned to IDTVA immediately.

- Inform the taxpayer a referral will be issued to an employee who will review and resolve the issue identified. Provide the appropriate timeframe and apology per IRM 25.23.2.2.3, *IDT Case Processing Time Frames*.
 - Update AMS narratives as applicable.
 - Forward the referral to the systemic approval path.
- (3) Paper - The presence of a TC 971 AC 123 PREPARER CONTACT on a taxpayer's entity does not confirm tax related identity theft but it does indicate that the taxpayer was a victim of identity theft. Complete research must be conducted to verify the taxpayer's claim. Identity theft returns resulting from a preparer data breach may appear to be duplicate or amended returns. These fraudulent returns may include:
- Duplicate or similar information to previously filed returns.
 - Income information that is consistent with the filing history and/or matches IRPTR data.
 - The same or similar tax preparer information.
 - Different refund/direct deposit information.
- (4) If a Form 14039 or police report is received, there is a TC 971 AC 123 PREPARER CONTACT on IDRS CC ENMOD/IMFOLE, and the only difference between the posted return and duplicate return is the refund/direct deposit information, consider the taxpayer submitting the identity theft claim to be the valid taxpayer. Follow applicable procedures within IRM 25.23.4, *IDTVA Paper Process*, to nullify the invalid return and address any other account conditions, as necessary.
- (5) If Form 14039 or police report is received, there is a TC 971 AC 123 PREPARER CONTACT on IDRS CC ENMOD/IMFOLE, and
- there is no difference between the posted return and duplicate return, the subsequent return is a true duplicate. If the name/address, dependents, income/credits, tax preparer/3rd party contact authorization, and refund/direct deposit/balance due information are all consistent with the filing history of the taxpayer **or**
 - if after researching the accounts you cannot find evidence of tax related identity theft affecting an account,
- a. Input TC 971 AC 506, BOD: WI, Program: AM, Tax Admin Code: OTHER
 - b. Secondary Date: use current filing tax year or tax year of duplicate return filing,
 - c. DO NOT INPUT A TC 971 AC 504, unless you have determined the taxpayer is a victim of income related identity theft not affecting tax administration.
 - d. Issue a Letter 4674C --Identity Theft Post-Adjustment Victim Notification Letter (IMF) I, 7, 8, w, y, and #. For international taxpayers use / in place of #.

Caution: If the TC 971 AC 506 is not input prior to cycle 47 of the processing year, an IP PIN/CP01A will not generate for the upcoming filing season. Use the following open paragraphs in addition to the paragraphs above. Paragraph 9: "Because we

processed your claim late in the year, we are unable to mail an IP PIN in December or January for this upcoming filing season. File your return as normal for this tax season. We will mail you an IP PIN next December or January. If your address changes before December, you will need to complete Form 8822, Change of Address. Visit www.irs.gov/form8822. Paragraph 1: "If you want an IP PIN to use for the upcoming tax year, visit our website at www.irs.gov/getanippin. A new IP PIN generates each year in mid-January. You can retrieve it by logging into your account at www.irs.gov/getanippin. If you chose to create an account to obtain an IP PIN, you will not receive a notice in December or January as stated above."

25.23.2.9
(10-01-2024)
**Identity Protection
Personal Identification
Number (IP PIN)**

- (1) The IP PIN is a six-digit number assigned to taxpayers to help prevent the misuse of their TIN (i.e., Social Security number or ITIN) on federal income tax returns. An IP PIN helps the IRS verify a taxpayer's identity and accept their electronic or paper tax return.
- (2) The IP PIN protects the taxpayer's account, even if they no longer have a filing requirement.
- (3) A new IP PIN is generated at the end of the year for use in the next processing year for any returns filed during the processing year. This includes the current tax year return and any prior tax year returns.
- (4) Since an IP PIN is assigned to a TIN, joint filers may each apply for or have their own IP PIN.
- (5) Since there is a limited number of combinations for an IP PIN, some individuals may have the same IP PIN as others.

25.23.2.9.1
(07-16-2024)
**Participating in the IP
PIN Program**

- (1) Participating in the IP PIN Program is voluntary for taxpayers who are not victims of tax-related identity theft.

Type of Enrollment	Description
Automatic Enrollment	Taxpayers who have been victims of tax-related identity theft will be placed into the IP PIN Program automatically. See IRM 25.23.2.9.1.1, <i>Automatic Enrollment in the IP PIN Program</i> , for more information
Individual Online Account	Online account where taxpayers can enroll in the IP PIN Program or display their IP PIN if already enrolled. See IRM 25.23.2.9.1.2, <i>Opting in to the IP PIN Program through the Individual Online Account</i> , for more information.

Type of Enrollment	Description
Form 15227, Application for an IP PIN	Taxpayers can apply for an IP PIN by submitting Form 15227. See IRM 25.23.3.2.7, <i>Application for an Identity Protection Personal Identification Number (IP PIN) Overview - Form 15227</i> , for eligibility.
Taxpayer Assistance Center (TAC) IP PIN Appointment	After taxpayers verify their identity in person at their local TAC, they are enrolled into the IP PIN Program. See IRM 25.23.2.9.1.3, <i>IP PIN TAC Appointment Procedures</i> , for when to make an appointment for the TP.

- (2) If the taxpayer voluntarily joined the IP PIN program, are not victims of tax-related identity theft and are not interested in continuing to participate in the program then they may opt-out of the IP PIN program. To find out if they are eligible to opt-out, please advise them to log into their online account, www.irs.gov/your-account.

25.23.2.9.1.1
(02-02-2023)
Automatic Enrollment in the IP PIN Program

- (1) Taxpayers are automatically enrolled into the IP PIN Program if their account contains a tax-related identity theft indicator, TC 971 AC 501 and/or TC 971 AC 506.
- (2) In cycle 20XX49, accounts without an IP PIN requirement are analyzed to determine if the account contains such an indicator. If so, an IP PIN is generated for the account and the IP PIN requirement is set.

#

25.23.2.9.1.2
(07-16-2024)
Opting into the IP PIN Program through the Individual Online Account

- (1) All individuals with an SSN or an ITIN are eligible to opt into the IP PIN program. They can opt in through their Individual Online Account at www.irs.gov/your-account. Individuals who do not already have an account must register by verifying their identity. Once enrolled, they can immediately view their IP PIN on the **Profile** page of their account.
- (2) Individuals need to know the following before applying for an IP PIN:
- Joint filers must each apply for their own IP PIN.
 - Most minor dependents will not be able to verify their identity online to get an IP PIN.
 - Once enrolled they must log into their account every year to retrieve their new IP PIN for that processing year.
 - Only individuals who voluntarily joined the IP PIN program, and who are **NOT** victims of tax-related identity theft may opt-out of the IP PIN program. See IRM 25.23.2.9.1(2) for more information.

Note: If the individual is unable to verify their identity to establish an online account, they may be eligible to use one of the alternative methods to opt in

to the IP PIN Program options listed in IRM 25.23.2.9.1, *Participating in the IP PIN Program*.

- (3) If you receive a call from an individual about issues with accessing the IP PIN through their online account, please provide the information below for the specific scenario:

If the individual is attempting to	Then
Retrieve their IP PIN Note: This is for individuals already part of the IP PIN population. This service is NOT for first time IP PIN applicants)	Refer to IRM 25.23.2.9.4.1 to determine if the taxpayer is eligible to have a Letter 4869C issued.
Enroll into the IP PIN Program and have received an identity theft letter that informs them that they will be receiving an IP PIN at the end of the year and invites them to enroll earlier if they choose to.	Inform the taxpayer that they will receive their IP PIN via CP01A by January. Also, inform them they can file their tax return normally, without an IP PIN, if they have not filed yet.
Enroll into the IP PIN Program and have received a notice inviting them to join the IP PIN Program or they are just trying to enroll.	Inform the taxpayer about the other options to enroll into the IP PIN Program. See IRM 25.23.2.9.1. Also inform the taxpayer, they can always file their return without enrolling into the IP PIN Program.

Reminder: Individuals may call asking when their IP PIN will generate online. The IP PIN for the **CURRENT** calendar year will be immediately available to them once they pass authentication and establish their online account. They will need to access their account each year to acquire their IP PIN to use for any filings during that calendar year.

Note: As of January 2019, any individual who enrolled in the IP PIN Program online, will need to access their online account every year, prior to filing, to get their new IP PIN for that processing year. Any individual who has enrolled into the IP PIN program prior to January 2019 will still receive a CP01A notice containing their IP PIN for the new processing year.

25.23.2.9.1.3
(05-08-2023)

IP PIN TAC Appointment Procedures

- (1) Taxpayers may call the IRS to request an appointment to obtain an IP PIN.
- (2) Do not schedule TAC appointments for taxpayers who are requesting a re-issuance of their IP PIN due to lost, misplaced, or non-receipt. Please refer to IRM 25.23.2.9.4.1, *Lost, Misplaced, or Non-Receipt of IP PIN*.

25.23 Identity Protection and Victim Assistance

- (3) Before offering to schedule an appointment, offer the taxpayer the alternative options available for obtaining an IP PIN. Please refer to IRM 25.23.12.6.2 (2), *Identity Protection Personal Identification Number (IP PIN) TAC Appointment Request Received on Toll-Free Account Lines (App 20/21, 161/162)*. If the taxpayer received a Letter 4403C, or other options are not applicable, or they insist on an appointment continue to paragraph 4 below.
- (4) Advise the caller two forms of identification must be presented at their TAC visit. Provide the taxpayer with the required forms of acceptable documents listed in IRM 25.23.12.6.2 (3), *Identity Protection Personal Identification Number (IP PIN) TAC Appointment Request Received on Toll-Free Account Lines (App 20/21, 161/162)*. Appointments for a dependent IP PIN will need identity documentation from both the authorized person requesting the IP PIN (parent or legal guardian) and identity documentation for the dependent. In addition, if the requester is a party other than a parent/guardian listed as custody parent on CC DDBKD, they will need to show proof of legal guardianship or custody.
- (5) If the caller is scheduling an appointment for both a primary and secondary taxpayer, each taxpayer must be present at the appointment and is required to present their own forms of identification.
- (6) If the caller is scheduling an appointment for a dependent IP PIN, the dependent does not need to be present for appointment, However, forms of identification for the dependent need to be brought to the TAC appointment along with their own identification documentation.
- (7) Once you have determined that an appointment is necessary and provided the information above, follow procedures in IRM 21.3.4.2.4, *Taxpayer Assistance Center (TAC) Appointment Service*.

25.23.2.9.1.3.1
(02-02-2023)

IP PIN TAC Procedures- (TAC Employees Only)

- (1) Authenticate the requester identity. If the request is for a dependent IP PIN, the parent/legal guardian must present documentation for themselves and the dependent. The dependent does not need to be present at the appointment. See table below for identity confirmation and examples of acceptable documents:

Note: If the taxpayer provides foreign documentation for picture identification, follow IRM 3.21.263.6.3.4.2, *Reviewing Supporting Identification Documents*, to determine if it is acceptable.

Identity Confirmation	Acceptable Documentation
<p>Individual must present a valid, current U.S. federal or state government issued form of picture identification such as:</p> <p>Note: In this instance, a valid, current U.S. federal or state government issued form includes the governments of the seven populated United States possessions: Puerto Rico, Guam, US Virgin Islands, Northern Mariana Islands, American Samoa, Midway Atoll and Palmyra Atoll. American Samoa and the country of Samoa are two separate political entities. The country of Samoa is NOT a US Possession.</p>	<ul style="list-style-type: none"> • A driver's license • State identification card • Passport <p>Reminder: Any current US federal or state government issued identification presented MUST be signed by the issuing agency and/or the individual where appropriate.</p>
<p>Individual must provide at least one additional form of identification such as:</p>	<ul style="list-style-type: none"> • A driver's license • State identification card • Passport • Social Security Card • Car Title • Voter Registration Card • Mortgage Statement • Lease agreement for rental domicile • Utility Bill matching address of ID • Birth Certificate (Requires Name at Birth, Date of Birth, and City of Birth) • School Records <p>Note: IRS no longer accepts Puerto Rican birth certificates issued before July 2010, due to new laws by the Government of Puerto Rico. Individuals with birth certificates issued before this date must get new documentation from the Puerto Rico Vital Statistics Record Office.</p>

- (2) If the request is for a dependent IP PIN, the requestor must show proof of identity (above) along with two forms of identity documents listed below for the dependents. If the requestor is a party other than a parent/guardian listed as custody parent on CC DDBKD, they must show proof of legal guardianship/custody.

Identity Confirmation for minor/dependent or certain religious groups	Acceptable Documentation
<p>Individual is a minor/dependent or member of a certain religious group (Amish, Mennonite or other), who do not have a photo identification because of their religious beliefs. must provide two forms of identification</p>	<ul style="list-style-type: none"> • Social Security card • State Identification card • Passport • Birth Certificate (Requires Name at Birth, Date of Birth, and City of Birth) • Bank Statements • Student Records (grade/ high school/college) <p>Note: Accept school records from the last year completed plus one other item from the list.</p> <ul style="list-style-type: none"> • Approved copy of Form 4029, Application for Exemption from Social Security and Medicare Taxes and Waiver of Benefits • Document (on Letterhead) from Health Care Provider (Doctor, Nurse or clinic) <p>Reminder: Document (on Letterhead) from Health Care Provider (Doctor, Nurse or clinic) must have ALL of the following information verifying identity of Taxpayer:</p> <ul style="list-style-type: none"> • Full Name of Taxpayer (including Parent or Guardian if minor/student) • Address, city, state, zip • Date of Birth • Date and Signature of Health Care Provider (doctor, nurse or clinic)

- (3) All documentation presented for identity verification must be notated on AMS history. **IF the request is for a dependent IP PIN, notate under the dependent SSN on AMS history and the requestor SSN (parent/legal guardian) on AMS history.**

Note: Please input the full name of both the dependent and the requesting parent/legal guardian on AMS history along with the complete current address.

- (4) If taxpayer did not pass identity verification either for themselves or their dependent or both, explain they should file as they normally would and file a return without an IP PIN. Notate on AMS History for each taxpayer who did not pass identity verification the reason why. If request for IP PIN was for a dependent, and the authorized person failed to pass identity authentication, notate this under both the requestor SSN and the dependent SSN on AMS.
- (5) If taxpayer passes authentication,
- Check IMFOLE for an IP PIN indicator, see IRM 25.23.2.9.2, *Identifying If a Taxpayer has an IP PIN Requirement*. If taxpayer has an IP PIN requirement, advise the taxpayer they are already enrolled in the IP PIN program and their TIN will be sent to the Identity Protection Group for processing and approval for an IP PIN re-issuance notice. If approved, a Letter 4869C containing their IP PIN will be issued, normally within 21 days.
 - Check the taxpayer's address on IDRS and update if applicable.
 - Access the *TAC IP PIN Request Tool* and enter the taxpayer's TIN.
 - Notate on AMS History if the taxpayer has an IP PIN requirement.
- (6) If the taxpayer does not have an IP PIN requirement then check the taxpayer's address on IDRS and update if applicable.
- (7) If the request is for a dependent or a first-time filer IP PIN, and there is no entity for the SSN, notate the first, middle and last name and complete address of the dependent/first time filer under that SSN on AMS history. If request is for a dependent, also notate under the parent/legal guardian requestor SSN on AMS history.
- (8) Advise the taxpayer the IP PIN request will be sent to the Identity Protection Group for final approval and processing. If approved an IP PIN will be assigned, and a CP01A notice with their IP PIN will be issued, normally within 3 weeks. The notice will contain all necessary information on how to use their IP PIN when filing their federal tax returns. Advise the taxpayer if they don't receive a notice with their IP PIN within 30 days, they will need to file normally without the IP PIN.
- (9) Access the *TAC IP PIN Request Tool* and enter the taxpayer's TIN.
- (10) Check to make sure the AMS history is notated with all required information. If the request is for a dependent IP PIN, both parent/legal guardian and the dependent AMS histories must be updated with the required information. Not entering the required information on AMS history could result in the IP PIN being denied.

25.23.2.9.2
(01-05-2021)

Identifying If a Taxpayer has an IP PIN Requirement

- (1) To determine if a taxpayer's account had an IP PIN generated, review CC IMFOLE for an IP PIN indicator. IMFOLE line 14 will display:

- **IP PIN:1** if an IP PIN was generated to the taxpayer's account.
- **IP PIN:0** if no IP PIN was generated to the taxpayer's account.

Note: Refer to Exhibit 2.3.51-13, *Command Code IMFOL Output Display — Entity*, for additional information.

Example: NYPTA: FMS CD: PDC-ID: ID THEFT 1:2 ID THEFT 2:0 IP PIN:1

- (2) IP PIN Indicator is set:

- In December for accounts that contain an unreversed tax-related IDT indicator without a previous IP requirement are automatically enrolled into the IP PIN Program and the IP PIN indicator is set to "1". **OR**
- At the time a taxpayer opts into the IP PIN Program. The IP PIN indicator is set to "1" when the opt in transaction posts to their account; TC 016 with DLN 28263-777-77777-Y. (Y signifies the year digit.)

25.23.2.9.3
(10-01-2024)

Receiving and/or Retrieving your Annual IP PIN

- (1) IP PINs are generated annually in early December for the upcoming processing year. IP PINs are generated for every TIN in the IP PIN population; however, some accounts will have an IP PIN generated but will not have a notice mailed.

- (2) **CP01A Notice** – This notice contains the taxpayer's IP PIN. It is mailed starting in Mid-December and should be received by Mid-January.

- (3) **Suppressed Notices** – Some accounts that have an IP PIN requirement do not have notices generated due to the following reasons:

- Taxpayer opted into the IP PIN Program in 2019 or later through the Get an IP PIN application or the Individual Online Account. CC ENMOD/IMFOLE will contain a TC 016 with the unique DLN of 28263-777-77777-Y (Y signifies the year digit.) with a cycle date of 201904 or greater.
- Taxpayer's account contains an undeliverable indicator. Review CC INOLES for 'UD' which displays on the second row.
- Taxpayer has not filed a return within the past 3 years.

Exception: A subsequent unreversed TC 971 AC 528 will bypass the non-filer suppression criteria.

- Taxpayer's account contains an unreversed IDT indicator with MISC code containing 'NOFR' and there has been no subsequent return filed.

#

- (4) If the taxpayer did not receive a CP 01A Notice, see IRM 25.23.2.9.4, **Lost, Misplaced or Non-Receipt of IP PIN Overview**.

- (5) Taxpayers who opted in online, must log into their Online Account to view their current IP PIN on the Profile page, see IRM 25.23.2.9.1.2, *Opting into the IP PIN Program through the Individual Online Account*.

Exception: Do not direct IP PIN requests for dependents to Online Service, most dependents will not be able to create an Online Account.

25.23.2.9.4

(06-17-2024)

Lost, Misplaced or Non-Receipt of IP PIN Overview

- (1) The *IP PIN Entry Tool* was developed to re-issue a taxpayer's IP PIN. The IP PIN Entry Tool will verify that an IP PIN was generated for the taxpayer for the current processing year. If an IP PIN was generated, it will transmit the TIN to Headquarters for processing of Letter 4869C which re-issues the IP PIN to the taxpayer.

Note: Only designated assistors can access the tool at *IP PIN Entry Tool*.

- (2) Do not suggest filing a Form 15227, Application for an Identity Protection Personal Identification Number (IP PIN), or schedule TAC appointments for taxpayers who are requesting a re-issuance of their IP PIN because it was lost, misplaced, or the IP PIN could not be retrieved through the Individual Online Account.
- (3) The IP PIN Entry Tool is taken offline for annual end of year maintenance period in November and brought back online in mid-January. Employees will not be able to input requests during this period. A SERP Alert will be issued when the Tool is active and available for use. If the taxpayer calls requesting that we re-issue their IP PIN during this maintenance period, please explain the following:
- The re-issuance process is offline for yearly maintenance and will be back online in mid-January.
 - They may file by paper, without an IP PIN at any time but it will delay the process of their return.
 - A digital copy of the CP01A notice is viewable in the **Notices** section of the Individual Online Account. Taxpayers with an account who received a CP01A may be able to retrieve their IP PIN, when the *IP PIN Entry Tool* is offline. See IRM 21.2.1.62(10), *Online Account*.

Reminder: Do not complete a Form 4442 during the maintenance period and do not suggest filing a Form 15227.

25.23.2.9.4.1

(06-17-2024)

Lost, Misplaced or Non-Receipt of IP PIN

- (1) If you receive a call regarding,
- A lost or misplaced IP PIN
 - Non-receipt of the CP01A containing the IP PIN
 - The IP PIN could not be retrieved through the Individual Online Account
 - Status of their IP PIN

Then follow the chart below for the appropriate authentication procedures:

Reminder: If the caller is unable to pass disclosure, **do not** refer them to the TAC appointment line or direct them to a TAC and **do not** suggest filing a Form 15227. Instead, inform the caller of the self-help methods in

paragraph 8 below. Explain to the caller that if they are unable to use the self-help methods to retrieve their IP PIN, they must file their tax return by paper, without an IP PIN.

If	Then
1. Taxpayer calls	Perform required and additional authentication on the taxpayer using the IAT Disclosure tool to assist callers. For more information see IRM 25.23.12.2, <i>Identity Theft Telephone General Guidance</i> .
2. Taxpayer's Spouse calls	Perform third party authentication using the IAT Disclosure tool. Follow guidance in IRM 21.1.3.3, <i>Third-Party (POA/TIA/F706) Authentication</i> . Reminder: If third-party disclosure is met the Letter 4869C can only be reissued to the taxpayer.
3. Taxpayer's Tax Professional or anyone authorized via the Form 8821 or Form 2848 calls	Perform third party authentication using the IAT Disclosure tool. Follow guidance in IRM 21.1.3.3, <i>Third-Party (POA/TIA/F706) Authentication</i> . Reminder: If third-party disclosure is met the Letter 4869C can only be reissued to the taxpayer.

If	Then
<p>4. Parent or Legal Guardian calls regarding their minor (under the age of 18) dependent's IP PIN</p>	<ol style="list-style-type: none"> 1. Perform required and additional authentication on the parent or legal guardian of the dependent using the IAT Disclosure tool. For more information see IRM 25.23.12.2, <i>Identity Theft Telephone General Guidance</i>. 2. Verify the identity of the parent or legal guardian using IDRS command code DDBKD to confirm the caller is the parent or legal guardian of the minor dependent for the current year. See IRM 25.23.12.2, <i>Identity Theft Telephone General Guidance</i>, for additional guidance when a call is received from a parent or legal guardian and IRM 2.3.80.4, <i>DDBKD Display Screen when Command Code Definer is 'space'</i> for guidance on researching and interpreting DDBKD information. 3. If research confirms parent or legal guardian then conduct Required Taxpayer Authentication with the parent/legal guardian, on the dependents TIN using the IAT Disclosure Tool. 4. If research determines the individual is not a parent or legal guardian, then follow procedures in box 2 of the chart for continuing to authenticate the individual using third-party authorization.

If	Then
5. Taxpayer calls regarding their adult (over the age of 18) dependent's IP PIN	<p>Perform third-party authentication using the IAT Disclosure tool. Follow guidance in IRM 21.1.3.3, Third-Party (POA/TIA/F706) Authentication.</p> <p>Reminder: If third-party disclosure is met the Letter 4869C can only be reissued to the taxpayer.</p>

Reminder: When receiving calls from someone other than the taxpayer, notate AMS with detailed history. Under the minor or individual's TIN, indicate the third-party individual whom you spoke with and indicate if authentication was pass/fail. See IRM 25.23.12.2, *Identity Theft Telephone General Guidance* for more information.

- (2) Confirm the taxpayer has an IP PIN requirement, see IRM 25.23.2.9.2, *Identifying If a Taxpayer has an IP PIN Requirement*.
- (3) Some accounts will not have the CP 01A listed because the notice was suppressed due to various reasons, see IRM 25.23.2.9.3, *Receiving and/or Retrieving your Annual IP PIN*.
- (4) Inform the taxpayer that we can re-issue their IP PIN via a Letter 4869C normally within 21 calendar days by mail, if the following is true:
 - The taxpayer's account is enrolled in the IP PIN program. See IRM 25.23.2.9.2, and
 - The taxpayer did not "opt in" to the IP PIN Program within the current calendar year. If the taxpayer opted in within the current calendar year, ENMOD/IMFOLE will contain a TC 016 with the unique DLN of 28263-777-7777-Y with a cycle posting date starting with the current calendar year (Y signifies the year digit.).
 - A CP01A **was not** issued prior to cycle 47 of the current calendar year.

Note: Taxpayers may request a change of address to receive Letter 4869C if they meet the criteria in IRM 21.1.3.20.1, *IMF and BMF Oral Statement Address Changes*. The address change **must** be input before the TIN is entered into the IP PIN Tool.

- (5) The following information and tables are for telephone assistors.

Caution: If the taxpayer is eligible to have their IP PIN re-issued, the steps in the table below **must be followed**, even if the taxpayer later decides to attempt to retrieve their own IP PIN via the self-help methods mentioned in paragraph 8.

If the IP PIN Tool is:	Then:
Available and the tool is online	<p>Input the taxpayer's TIN into the IP PIN Entry tool:</p> <ul style="list-style-type: none"> • Response - "XXX-XX-XXXX has been saved for processing." TIN successfully saved for processing • Response – "PY 20XX IP PIN was not generated for XXX-XX-XXXX". <p>If the response indicates an unsuccessful attempt, check to ensure the TIN was input correctly, if:</p> <ul style="list-style-type: none"> • not correct – re-input TIN • correct – taxpayer was not enrolled in the IP PIN Program or has opted-in within the current year; taxpayer is not eligible for re-issuance. Inform the taxpayer they do not meet the re-issuance criteria and that they must file by paper if they are unable to use the self-help methods to retrieve their IP PIN.
Not available or offline	<p>Complete Form 4442 and forward it to your Lead.</p> <p>Reminder: Do not complete a Form 4442 during the maintenance period.</p>

Reminder: Inform the taxpayer that at any time they can file their return by paper. Inform the taxpayer that if they do not receive their re-issued IP PIN letter within 21 calendar days, or if they do not meet the requirements in the list above, or are unable to use the self-help methods in paragraph 8 below, filing by paper would be their only option. A paper return with a missing or incorrect primary and/or secondary taxpayer IP PIN is subjected to additional review for identity verification, which will delay return processing and issuance of any refund that may be due.

- (6) Consolidation of Forms 4442 for Processing - Using established local procedures, the TINs from all completed Forms 4442 for each site will be input into the IP PIN Entry Tool within 48 hours. As the TINs are input into the IP PIN Entry Tool, one of two responses will be displayed.

If the response states:	Then
TIN saved for processing.	TIN has been transmitted to Headquarters for processing.
PY 20XX IPPIN was not generated for XXX-XX-XXXX	<p>Check to ensure the TIN was input correctly, if:</p> <ul style="list-style-type: none"> not correct – re-input TIN correct – taxpayer was not enrolled in the IP PIN Program or has opted-in within the current year; taxpayer is not eligible for re-issuance. Reject the Form 4442 back to the submitter with instructions to add history on AMS stating the taxpayer doesn't qualify to have an IP PIN reissued.

- (7) If the taxpayer contacts you regarding the non-receipt of the Letter 4869C, research their account to determine if the taxpayer was eligible to receive an IP PIN. If a letter was sent, CC ENMOD will have the history item "4869C" with an IDRS number of 1387800000.

If research reveals the taxpayer:	Then advise the taxpayer:
was eligible to receive the letter and the letter was sent	<ul style="list-style-type: none"> What date our records indicate the letter was sent. If within 21 calendar days, they may still receive the letter. If beyond 21 calendar days, then filing by paper without an IP PIN would be the only option. Apologize for the inconvenience.
was eligible to receive the letter and the letter was not sent	<ul style="list-style-type: none"> That filing by paper without an IP PIN would be the only option. Apologize for the inconvenience.
was not eligible to receive the letter	<ul style="list-style-type: none"> They must file by paper without an IP PIN. Apologize for the inconvenience.

- (8) Inform the taxpayer that they may obtain/view their IP PIN faster by accessing their Individual Online Account located online at *IRS.gov/your-account*. See IRM 21.2.1.62(10), *Online Account*. The IP PIN will be viewable on the **Profile** page of their account. Also, a digital copy of the CP 01A containing their IP PIN may be available in the **Notices** section of their account.

Exception: Most minor dependents will not be able to establish an Individual Online Account. Do not direct the taxpayer to online services to obtain their IP PIN for their minor dependent or if the account has an unreversed TC 971 AC 527 on CC ENMOD/IMFOLE.

Note: The Get an IP PIN application is not available during the end of year maintenance period, see IRM 25.23.2.9.4, *Lost, Misplaced or Non-Receipt of IP PIN Overview*.

- (9) Remind the taxpayer if they change their address prior to the next filing season, they must complete Form 8822, *Change of Address* (available by visiting *www.irs.gov/f8822*) prior to the start of the next tax season to receive their CP 01A notice. 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.

25.23.2.9.5
(01-20-2022)

Filing Returns with an IP PIN

- (1) Taxpayers issued an IP PIN are required to use the IP PIN when filing their return, to avoid delays and rejection.

(2) **Electronic Filing –**

- Taxpayers filing electronically will be prompted by their software program to input their IP PIN and the IP PIN of anyone else on the return with a requirement. The input of the IP PIN varies with the different software programs.

Caution: If a taxpayer states that they cannot locate where to input their IP PIN using their tax software, they should contact the software provider. IRS cannot help with individual software issues.

Note: An e-file return will reject and not be processed if a required IP PIN is missing or incorrect.

- Entry of an IP PIN will be required for any Taxpayer Identification Number (TIN), including all Social Security Numbers (SSNs) and Individual Taxpayer Identification Number (ITINs) with an IP PIN requirement including dependents being claimed on Form 2441, Child and Dependent Care Expenses; and Schedule Earned Income Tax Credit (EITC)
- If a taxpayer contacts the service stating their electronic filing rejected due to prior use of their (TIN) even though they used their IP PIN: apologize for the inconvenience, tell the taxpayer to file a paper return using their IP PIN and do not make any statements about the IP PIN Program beyond your apology.

(3) Paper Filing

- The primary taxpayer filing on a paper Form 1040 with an IP PIN must enter the IP PIN in the boxes indicated just to the right of the "Your Occupation" space in the signature section of the form. If the secondary taxpayer, if they have an IP PIN must when filing on paper enter the IP PIN in the indicated box, just to the right of the Spouse's Occupation space in the signature section of the form.

Reminder: If the dependent has an IP PIN assigned, there is currently no requirement to enter this information on a paper return.

- 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.

Note: If the Taxpayer has questions about completing their return, see Instructions Table of Contents for a list of instructions for the Form and Schedules.

25.23.2.10 (09-12-2019) Get Transcript Breach

- (1) During filing Season 2015, third parties gained unauthorized access to the "Get Transcript" online application using taxpayer Personally Identifiable Information (PII) they obtained through sources outside IRS. You can identify these taxpayers by reviewing ENMOD/IMFOLE for a TC 971 AC 505 with one of the following three breach numbers:

- TC 971 AC 505 IR20150521512
- TC 971 AC 505 IR20150521555
- TC 971 AC 505 IR20150521556

- (2) Taxpayer accounts previously disabled from the Secure Access application due to the Get Transcript breach prior to May 2016, such as the Get Transcript Incident, have been opened and the taxpayer can now access the application. Accounts that remain disabled in Secure Access can be identified by an unreversed TC 971 AC 527 WI BREACH DSABLD on the entity. If there is an unreversed AC 527 on the account, See IRM 25.23.2.8.6, *Disabled Online Accounts TC 971 AC 527*.

25.23.2.11 (12-10-2019) Get an Electronic Filing PIN Incident

- (1) Third parties gained unauthorized access to the "Get Your Electronic Filing PIN" online application using taxpayer Personally Identifiable Information (PII) they obtained through sources outside IRS. There was no disclosure of PII by the IRS and the IRS is taking additional steps to prevent a fraudulent return from posting to the taxpayer's account. The IRS developed methods to identify these accounts using TC 971 AC 505.
- (2) In June of 2017, the IRS announced the discontinuance of the e-File PIN application. As a result, the IRS will no longer accept the e-file PIN as a variable for validating returns. Taxpayers will now be required to use their prior year Self-Select PIN (SSP) or their prior year Adjusted Gross Income (AGI) to sign and

25.23 Identity Protection and Victim Assistance

validate their returns. Taxpayers seeking their AGI may acquire this information through Get Transcript Online or Order a Transcript by Mail (web and phone applications).

- (3) IRS grouped the unauthorized access accounts into three populations and developed coding to facilitate case recognition.
 - IR20160127510 Successfully obtained E-File PIN
 - IR20160127513 Unsuccessfully attempted to obtain E-File PIN
 - IR20160614508 (this number designates a separate incident and identifies both successful and unsuccessful attempts.)

Note: Affected accounts are blocked from on-line applications. These taxpayers will **NOT** be able to log into on-line accounts or services (for example: Get Transcript, IP PIN and Online Payment Agreement (OPA) due to the fraud incident. As access to OPA is not available, CSRs will assist taxpayers who wish to establish an installment agreement, refer to IRM 5.14.5.2, *Streamlined Installment Agreements*, for additional information on installment agreements.

- (4) Taxpayer accounts previously disabled from the Secure Access application due to the Get an Electronic Filing PIN breach prior to May 2016, have been opened and the taxpayer can now access the application. Accounts that remain disabled in Secure Access can be identified by an unreversed TC 971 AC 527 WI BREACH DSABLD on the entity. If there is an unreversed AC 527 on the account, See IRM 25.23.2.8.6, *Disabled Online Accounts TC 971 AC 527*.

25.23.2.12
(09-12-2019)

Free Application for Federal Student Aid (FAFSA) Breach

- (1) Between January, 2017 and March, 2017, third parties gained unauthorized access to the IRS Data Retrieval Tool (DRT) that is accessed from the Department of Education's Free Application for Federal Student Aid (FAFSA) website to retrieve tax information for student loan applications and repayment plans, using taxpayer Personally Identifiable Information (PII) they obtained through sources outside IRS. The individuals can be identified by reviewing ENMOD/IMFOLE for a TC 971 AC 505 with breach number CR20170228961 and a secondary date of 01/31/2017. A history item was placed on IDRS.
- (2) DRT is now available. The individuals whose information may have been accessed were sent letters (4281C). The letter notified these individuals that their personal identity information and tax data could be at risk. It also provided guidance on how to enroll for free identity theft protection for one year through Equifax and how to obtain an Identity Protection Personal Identification Number (IP PIN).

Note: Affected accounts are **NOT** blocked from on-line applications. These taxpayers will be able to log into on-line accounts and services (for example: Get Transcript, IP PIN and Online Payment Agreement (OPA)

- (3) If you receive questions about these letters, advise individuals to file as normal (if applicable) and follow the instructions in the letter they received. For additional guidance, see IRM 10.5.4, *Incident Management Program*.

25.23.2.12.1
(09-15-2020)
FAFSA Breach-CP302

- (1) Each day a taxpayer's account in the IRS Data Retrieval Tool (DRT) is accessed, the IRS will issue a CP302 to notify the taxpayer.
- (2) If the taxpayer calls about the receipt of a CP302, explain that they will receive a notice each day the DRT is accessed using their information. Probe the caller to ascertain if the taxpayer, or their parent, guardian, representative, etc. made the access.
- (3) Full disclosure and authentication are required for account related calls only. See IRM 21.1.1.4 (4), *Communication Skills*, for more information.

Note: When a taxpayer or third party contacts the IRS, and is only requesting general information regarding the CP302, authentication is not required. Information that is contained within the CP302 or on IRS web pages is considered public information and can be provided without authentication.

- (4) If the caller states that the access was not made by them, or by anyone on their behalf, take the following actions:
 - a. Advise the taxpayer of actions to take to protect their identity. See IRM 25.23.2.2.1, *Taxpayer Interaction*, for a list of actions.
 - b. TC 971 AC 522 with MISC Code of OS PHSB IRSID and
 - c. TC 971 AC 504 with MISC Code of NKI

Note: Use the date of one day prior to contact as the Secondary Date for the TC 971 input on both AC 522 and AC 504. Per Exhibit 25.23.2-4, *IMF Only TC 971 AC 504*, one AC 504 per account (not year or incident) is sufficient.

Caution: Take these actions on the account only if the caller is sure the access was not made by taxpayer or anyone on their behalf for example their parent, guardian or representative, etc.

25.23.2.13
(12-10-2019)
**Breach Numbers
CR20170421067 and
LR20170421067**

- (1) Third parties gained unauthorized access to an online application using taxpayer Personally Identifiable Information (PII) they obtained through sources outside IRS. You can identify these taxpayers by reviewing ENMOD/IMFOLE for a TC 971 AC 505 with the breach number CR20170421067 or LR20170421067 with a Breach Date of 3/30/2017. Letter 4281C was issued to the taxpayers impacted by the incident.
- (2) Taxpayer accounts previously disabled from the Secure Access application due to this breach prior to May 2016, have been opened and the taxpayer can now access the application. Accounts that remain disabled in Secure Access can be identified by an unreversed TC 971 AC 527 WI BREACH DSABLD on the entity. If there is an unreversed AC 527 on the account, See IRM 25.23.2.8.6, *Disabled Online Accounts TC 971 AC 527*.

25.23.2.14
(12-10-2019)
Form 8821 Breach

- (1) These accounts are identified by breach number LR20170425509. The taxpayers affected by this breach have been notified via Letter 4281C.
- (2) The majority of the accounts do not have their online account blocked, but there are a few whose on-line accounts are currently blocked from another breach, for example Get Transcript or Efile PIN.

- (3) Taxpayer accounts previously disabled from the Secure Access application due to this breach prior to May 2016, have been opened and the taxpayer can now access the application. Accounts that remain disabled in Secure Access can be identified by an unreversed TC 971 AC 527 WI BREACH DSABLD on the entity. If there is an unreversed AC 527 on the account, See IRM 25.23.2.8.6, *Disabled Online Accounts TC 971 AC 527*.
- (4) The victims with blocked accounts were told that they need to file a Form 14039 if they would like to obtain an IP PIN. Those taxpayers not blocked were sent instructions to OPT-IN for an IP PIN on-line if they so choose.

25.23.2.15
(12-06-2022)
**Identity Theft Liaison
Responsibilities**

- (1) An Identity Theft (IDT) Functional Liaison is representative of their function. The Liaison's name, contact phone and fax number are listed on the IDT Functional Liaison listing located on Servicewide Electronic Research Program (SERP). IDTVA Employees refer to this listing to identify a point of contact (POC) for referral purposes.
- (2) Processes which require referrals from the IDTVA IPSU staff to the functions for action include:
 - Form 14027-B, Identity Theft Case Referral, which is currently used exclusively for Global Review (GRVW) referrals.
- (3) IDT Liaisons will receive cases by secure e-mail or through CII.
- (4) IDT Liaisons will process identity theft referrals as priority. All cases involving identity theft will receive priority treatment. This includes functions not located within the IDTVA framework.

25.23.2.15.1
(12-06-2022)
**Functional
Responsibilities in
Receipt of Global
Review (GRVW)
Referrals**

- (1) Employees will receive Form 14027-B, Identity Theft Case Referral, through their designated IDT Liaisons to resolve a tax related issue involving identity theft whether or not there is an open control for the case on IDRS or CII.
- (2) Employees can identify cases related to Form 14027-B on AMS/CII and their Automated Age Listing (AAL) by a multiple control with a case controlled with Category Code GRVW and a Priority Code 1 on the IDT control.
- (3) Use the step chart below when a Form 14027-B is received.

Step	Action
1	Review sections I and II of F14027-B to ensure the tax related identity theft issue has been forwarded to the correct IDT liaison.

Step	Action
2	Acknowledge receipt of the form within 5 business days by filling out Section V on page 2 of the form and notating receipt of Form 14027-B on IDRS or AMS. Exception: SB/SE Field examiners do not use IDRS or AMS. These examiners use their normal case history worksheet to notate receipt of Form 14027-B.
3	Provide status updates to the taxpayer (interim letters or phone calls).
4	Record periodic status updates or enter history items (every 45 days) on IDRS or AMS.
5	Complete Form 14027-B through VIII when the case is resolved and closed.
6	Return the completed Form 14027-B to the IDTVA-I case-worker through the IDT Liaison, when applicable, upon resolution of the case.

This Page Intentionally Left Blank

Exhibit 25.23.2-1 (11-07-2019)

Acronyms and Definitions

The following tables describe the terms and acronyms used for the TC 971 AC 501, 504, and 506 identity theft indicator codes. The three tables are: 1) BOD/Function, 2) Program Name, and 3) Tax Administration Source. Not all Tax Administration Source Codes are available to all BOD/Functions. For specific BOD/Function information, refer to the applicable Exhibit for the Action Code, for example TC 971 AC 501 or AC 506.

1. BOD/Function

Term/Acronym	Description
AP	Appeals
CI	Criminal Investigation
LBI	Large Business & International
IT	Information Technology
OS	Operations Support
PPDS	Identity Protection Strategy & Oversight formerly Privacy, Governmental Liaison & Disclosure
SBSE	Small Business / Self-Employed
TAS	Taxpayer Advocate Service
TS (formerly WI)	Taxpayer Services (formerly Wage & Investment)

2. Program Name

Term/Acronym	Description
ACS	Automated Collection System
AM	Accounts Management (IRS or TP identified identity theft)
AMTAP	Return Integrity & Verification Operations (RIVO) formerly Accounts Management Taxpayer Assurance Program (AMTAP)
AP	Appeals
ASFR	Automated Substitute for Return
AUR	Automated Underreporter
CA	TAS Case Advocate
CFBALDUE	SB/SE: Field Collection - Taxpayer Delinquency Accounts
CFDELRET	SB/SE: Field Collection - Taxpayer Delinquency Investigations
CONGINQ	Congressional Inquiry

Exhibit 25.23.2-1 (Cont. 1) (11-07-2019)

Acronyms and Definitions

Term/Acronym	Description
CORR	SB/SE Correspondence Exam
CSCO	Compliance Services Collection Operations
CSIRC	Computer Security Incident Response Center
EXAM	TS Correspondence Exam
FA	Field Assistance
FO	Field Office
FLDEXAM	Field Exam
FLDADV	Field Advisory
FLDINSLV	Field Insolvency
RIVO	Return Integrity & Verification Operations
LBI	Large Business & International
OPIP	Identity Protection Strategy & Oversight
PHSH	Phishing
PREREF	Pre-Refund Program
PRP	Pre-refund Program
RC	Refund Crimes
RFND	Refund Scheme
RICS	Return Integrity & Compliance Services
SP	Submission Processing
TDI	Tax Delinquency Investigation
TEFRA	Tax Equity and Fiscal Responsibility Act of 1982
WHC	Withholding Compliance

3. Tax Administration Source

Note: The new MISC codes that contain an “M” next to them identify cases requiring a manual 4402C instead of a new systemic notice (CP01C (English) and CP701C (Spanish)). The new notices will be issued once the TC 971 AC 504 and original MISC codes posts to the TP’s account.

Term/Acronym	Description
ACCT and ACCT-M	Non-tax-related issues: One or more personal accounts have been opened under the victim’s identity or the victim reported questionable account activity.
BOTH and BOTH-M	Non-tax-related issues: Both EMPL and ACCT

Identity Protection and Victim Assistance - General Case Processing 25.23.2

page 105

Exhibit 25.23.2-1 (Cont. 2) (11-07-2019)

Acronyms and Definitions

Term/Acronym	Description
DDb	Used by RICS Pre-Refund for cases selected by DDb filter and identified as an Identity Theft return
DECD	Taxpayer is deceased
EAFail	Non-tax-related issue: Used exclusively by RICS for situations where the Electronic Filing PIN (EFP) Application has been linked to a telephone line which has been blocked after a series of attempts to secure a PIN
EMPL and EMPL-M	Non-tax-related issue: Victim's SSN Used for Employment.
ERC027	Primary Taxpayer under 14 years old
IDT	Used by RICS Pre-Refund for CI Cases where a bad return was filed under the taxpayer's SSN
INCOME	Identity theft identified and substantiated due to an underreporting of income
IRSID	During the normal course of business, the IRS suspects identity theft may have occurred, and the case is not yet resolved.
MULTFL	Identity theft identified and substantiated due to two or more tax returns filed for one taxpayer
INCMUL	Identity theft identified and substantiated due to both underreporting of income and multiple filings
NKI and NKI-M	No known taxpayer impact
NOFR	Substantiated identity theft incidents where the victim does not have a filing requirement
OTHER	Identity theft which cannot be identified as related to any existing Tax Administration Source types
OTHER1	Used by RICS to identify an SSN where there is at least one good return filed with a valid address
PNDCLM	The taxpayer makes an initial claim of identity theft. They have not yet submitted their claim.
PRISNR	Taxpayer is incarcerated
RFND	Identity theft identified by the filing of a false return in order to obtain a refund
SSA	Used by RICS Pre-Refund for cases identified by SSA filters, but are confirmed Identity Theft cases
RPM1, RPM2, RPM3, RPM4	Used by AM and Compliance functions to flag Return Preparer Misconduct cases. Employees will notify these taxpayers that the Service will provide identity protection via the IP PIN as they are vulnerable because of their dealings with a bad preparer.

Exhibit 25.23.2-1 (Cont. 3) (11-07-2019)**Acronyms and Definitions**

Term/Acronym	Description
SPCL1	Applied when there is at least one incident of failed High-Risk Disclosure during a phone call and a taxpayer is requesting their Adjusted Gross Income (AGI) or Self Select PIN (SSP) so that they can e-file their tax return
SPCL2	TC 971 AC 504 SPCL2 will be applied to a taxpayer's SSN when the taxpayer alleges BMF ID theft that is affecting their SSN. Prior to January 2015, used by AM and Compliance functions to flag Return Preparer Misconduct cases. Employees will notify these taxpayers that the Service will provide identity protection via the IP PIN as they are vulnerable because of their dealings with a bad preparer.
UNAUDP	Unauthorized use of a dependent person
UNWORK	An identity theft claim has been received but has not been resolved yet. See Exhibit 25.23.1-1, <i>Glossary of Identity Protection Terms and Definitions</i> , for more information.
UPC147	Input on the identified IRSN corresponding to the non-legitimate unpostable return with UPC147 RC 1 as identified and determined by SP
UPCMUL	Input on true SSN owner's account when a non-legitimate unpostable return with UPC147 RC 1 has been filed using the taxpayer's SSN as identified and determined by SP

Identity Protection and Victim Assistance - General Case Processing 25.23.2

page 107

Exhibit 25.23.2-2 (10-01-2024)

IMF Only TC 971 AC 501 — Taxpayer Initiated Identity Theft Case Closure (Tax-Related) - TC 971 AC 501

The exhibit below demonstrates how IDTVA inputs a TC 971 AC 501 when the taxpayer is a victim of income related identity theft affecting tax administration.

```
FRM77 XXX-XX-XXXX    MFT>00    TX-PRD> 000000    PLN-NUM>    NM-CTRL> XXXXXX
TC>971    TRANS-REGISTER-IND> PSTNG-DLAY-CD>
EXTENSION-DT>    TC93X-EMP-CD>    TRANS-DT>
CLOSING-CD>    RESP-UNIT/JURISDICTION-CD>    TC148-CD>
DLN-CD>    BL-LOC-CD>    LAST-RET-AMT-CD>    TC480-SC-CD>
CYCLE>    APP-OFF-CD>    CSED-CD>    BOD-CD>    BOD-CLIENT-CD>
SEQ-NUM>    REVERSAL-DLN>    SECONDARY-DT>12312009
CAF-CD>    TC971/151-CD> 501    TC550DEFINER-CD>    FEMA-NUM>
ULC>    FREEZE-RELEASE-AMT>    ABA-NUM>
TC46X-GRP-CD>    TC583-DEFINER-CD>
XREF-TIN>    XREF-NM-CTRL>
XREF-TIN-PRD>    XREF-PLN-NUM>    XREF-MFT>    MISC>WI AUR INCOME
CORR-DT-IND>    REFILE-LIEN-*IND>    2032-IND>
REMARKS: Identity Theft
```

Input instructions for TC 971 AC 501 are as follows:

1. Obtain the following information:
 - Entity - SSN;
 - Business Operating Division (BOD)/Function (See Exhibit 25.23.2-1, *Acronyms and Definitions*;
 - Program Name (See table in (7) below);
 - Tax Administration Source (See Exhibit 25.23.2-1, *Acronyms and Definitions*; and
 - Tax Year affected by identity theft (Secondary-DT Field).

Note: The tax year affected by the identity theft **cannot** be the current year. For example, the taxpayer gave you a valid claim during the current year, for a 2012 tax year issue. You have resolved the issues, verified and updated the address. You will input TC 971 AC 501 for tax year 2012 by entering 12312012 in the Secondary-DT field on FRM77.

2. The tables provided below display the available Tax Administration Source Codes by BOD/Function/Program. Do not attempt to use Tax Administration Source Codes not listed for your BOD/Function (Program).
3. Navigate to CC FRM77
 - Sign into IDRS
 - Enter ENMOD (SSN), then press ENTER
 - Enter CC REQ77
 - CC FRM77 is displayed for the selected SSN

Caution: The Secondary Date field on CC REQ77 is limited to the current calendar year (cannot be the current day or any future date) and 7 prior years. The secondary date field will not allow the input of any date outside that range. See IRM 25.23.2.3.8.1, *Command Code REQ77 Secondary Date and Old Case Year Issue* for more information.

4. Enter the TC 971 AC 501
 - Enter the TC with 971
 - TRANS-DT is auto populated with the current date

Exhibit 25.23.2-2 (Cont. 1) (10-01-2024)**IMF Only TC 971 AC 501 — Taxpayer Initiated Identity Theft Case Closure (Tax-Related) - TC 971 AC 501**

- Enter SECONDARY-DT (enter the tax year affected by the identity theft incident in the format MMDDYYYY)
- Enter MISC (enter your specific BOD/Function, Program Name, and Tax Administration Source, see Exhibit 25.23.2-1, *Acronyms and Definitions*)
- After REMARKS, enter “IDENTITY THEFT”

5. Tax Administration Source Codes for use with TC 971 AC 501 - Taxpayer Identified Case Closure

Note: Taxpayers affected by Get Transcript breach will be flagged with TC 971 AC 506 WI AM OTHER.

You can identify these taxpayers by reviewing CC ENMOD for a TC 971 AC 505 IR20150521512, TC 971 AC 505 IR20150521555 or TC 971 AC 505 IR20150521556

Tax Administration Source Code	Definition of Tax Administration Source Code
ALTRD	Identity theft identified and substantiated due to an altered return
INCOME	Identity theft identified and substantiated due to an underreporting of income
MULTFL	Identity theft identified and substantiated due to two or more tax returns filed for one taxpayer
INCMUL	Identity theft identified and substantiated due to both underreporting of income and multiple filings
OTHER	Identity theft which cannot be identified as related to any existing Tax Administration Source types
NOFR	Identity theft identified by the filing of a false return in order to obtain a refund and the victim does not have a filing requirement
DECD	Deceased taxpayer
PRISNR	Incarcerated Taxpayer
REFCCA	IDTVA use only - Used for additional impacted years identified through Complete Case Analysis when the taxpayer has been determined to be a victim of refund related identity theft.
ICMCCA	IDTVA use only – Used for additional impacted years identified through Complete Case Analysis when the taxpayer has been determined to be a victim of income related identity theft affecting tax administration.

6. Do not attempt to use a Tax Administration Source Code that your BOD/Program (Function) is not profiled to use. The following table identifies the BOD/Programs and applicable Tax Administration Source Codes. Refer to Exhibit 25.23.2-1, *Acronyms and Definitions*, for definitions of the Program Name codes.
7. Appeals is profiled to use the following codes:

Identity Protection and Victim Assistance - General Case Processing 25.23.2

page 109

Exhibit 25.23.2-2 (Cont. 2) (10-01-2024)

IMF Only TC 971 AC 501 — Taxpayer Initiated Identity Theft Case Closure (Tax-Related) - TC 971 AC 501

BOD Name	Program Name	TC 971 AC 501 Tax Administration Source Code
AP	AP	INCOME, MULTFL, INCMUL, OTHER, NOFR, and DECD

8. Criminal Investigation is profiled to use the following codes:

BOD Name	Program Name	TC 971 AC 501 Tax Administration Source Code
CI	FO	INCOME, MULTFL, INCMUL, OTHER, NOFR, PRISNR, and DECD
CI	RC	INCOME, MULTFL, INCMUL, OTHER, NOFR, PRISNR, and DECD

9. Large Business & International is profiled to use the following codes:

BOD Name	Program Name	TC 971 AC 501 Tax Administration Source Code
LBI	LBI	INCOME, INCMUL, MULTFL, OTHER, NOFR, PRISNR, and DECD

10. IT is profiled to use the following codes:

BOD Name	Program Name	TC 971 AC 501 Tax Administration Source Code
MIT	CSIRC	DECD, OTHER, NOFR, and PRISNR

11. IPSO is profiled to use the following codes:

BOD Name	Program Name	TC 971 AC 501 Tax Administration Source Code
PPDS	CONGINQ	INCOME, MULTFL, INCMUL, OTHER, NOFR, PRISNR, and DECD
PPDS	OPIP	INCOME, MULTFL, INCMUL, OTHER, NOFR, PRISNR, and DECD

12. SBSE is profiled to use the following codes:

Exhibit 25.23.2-2 (Cont. 3) (10-01-2024)

IMF Only TC 971 AC 501 — Taxpayer Initiated Identity Theft Case Closure (Tax-Related) - TC 971 AC 501

BOD Name	Program Name	TC 971 AC 501 Tax Administration Source Code
SBSE	CFBALDUE	ALTRD, INCOME, MULTFL, INCMUL, OTHER, NOFR, PRISNR, and DECD
SBSE	CFDELRET	ALTRD, INCOME, MULTFL, INCMUL, OTHER, NOFR, PRISNR, and DECD
SBSE	FLDEXAM	ALTRD, INCOME, MULTFL, INCMUL, OTHER, NOFR, PRISNR, and DECD
SBSE	FLDADV	INCOME, MULTFL, INCMUL, OTHER, NOFR, and DECD
SBSE	FLDINSLV	INCOME, MULTFL, INCMUL, OTHER, NOFR, and DECD

13. TS is profiled with the following codes:

BOD Name	Program Name	TC 971 AC 501 Tax Administration Source Code
WI	ITVAA	INCOME, MULTFL, INCMUL, OTHER, NOFR, REFCCA and ICMCCA
WI	ITVAC	INCOME, MULTFL, INCMUL, OTHER and NOFR
WI	IP	ALTRD, DECD, INCMUL, INCOME, MULTFL, NOFR, OTHER, PRISNR, MISC1, MISC2, MISC3, MISC4 and MISC5
WI	RICS	INCOME, MULTFL, OTHER, NOFR, PRISNR, and DECD
WI	PREREF	INCOME, MULTFL, INCMUL, OTHER, NOFR, PRISNR, and DECD

Identity Protection and Victim Assistance - General Case Processing 25.23.2

page 111

Exhibit 25.23.2-3 (10-01-2018)

#

The exhibit below demonstrates how ACS inputs a TC 972 AC 501 when they determine identity theft was indicated by IRS in error.

```
FRM77 XXX-XX-XXXX    MFT>00    TX-PRD> 000000    PLN-NUM>    NM-CTRL> XXXXXX
TC>972    TRANS-REGISTER-IND> PSTNG-DLAY-CD>
EXTENSION-DT>    TC93X-EMP-CD>    TRANS-DT>
CLOSING-CD>    RESP-UNIT/JURISDICTION-CD>    TC148-CD>
DLN-CD>    BL-LOC-CD>    LAST-RET-AMT-CD>    TC480-SC-CD>
CYCLE>    APP-OFF-CD>    CSED-CD>    BOD-CD>    BOD-CLIENT-CD>
SEQ-NUM>    REVERSAL-DLN>    SECONDARY-DT>12312009
CAF-CD>    TC971/151-CD> 501    TC550DEFINER-CD>    FEMA-NUM>
ULC>    FREEZE-RELEASE-AMT>    ABA-NUM>
TC46X-GRP-CD>    TC583-DEFINER-CD>
XREF-TIN>    XREF-NM-CTRL>
XREF-TIN-PRD>    XREF-PLN-NUM>    XREF-MFT>    MISC>WI ACS IRSERR
CORR-DT-IND>    REFILE-LIEN-*IND>    2032-IND>
REMARKS: Identity Theft marked in error
```

Input instructions for TC 972 AC 501 are as follows:

1. Obtain the following information:
 - Entity - SSN
 - BOD/Function
 - Program Name (see Exhibit 25.23.2-1, *Acronyms and Definitions*)
 - Tax Year of the TC 971 AC 501 being reversed

Note: The tax year must match the tax year of the TC 971 AC 501 that is being reversed.

 - Transaction date of the TC 971 AC 501 being reversed
2. Navigate to CC FRM77
 - Sign into IDRS
 - Enter ENMOD SSN, then press ENTER
 - Enter CC REQ77
 - CC FRM77 is displayed for the selected SSN
3. Enter the TC 972 AC 501
 - Enter the TC with 972
 - Enter TRANS-DT (enter the transaction date of the TC 971 AC 501 being reversed)
 - Enter SECONDARY-DT (enter the tax year of the TC 971 AC 501 being reversed in the MMDDYYYY format)
 - Enter MISC (Modify the Reason Code field with the reason for the reversal). Select the Reason code that reflects the reason for the reversal from the options below
 - Enter REMARKS (enter your remarks)

Note: See Exhibit 25.23.2-2, *IMF Only TC 971 AC 501 — Taxpayer Initiated Identity Theft Case Closure (Tax-Related) - TC 971 AC 501*, for Secondary Date limitations and other necessary input. For more information on CC REQ77 see IRM 2.4.19, *Command Codes REQ77, FRM77 and FRM7A*, or the *IDRS Command Code Job Aid*.

Exhibit 25.23.2-3 (Cont. 1) (10-01-2018)

#

4. Tax Administration Source Codes for use with TC 972 AC 501 - Reversal of TC 971 AC 501 - are as follows:

TC 972 AC 501 Tax Administration Source Code	Definition
TPRQ	The taxpayer requests the 971 be reversed.
IRSERR	The 971 was due to a typographical mistake or another internal mistake.
IRSADM	The 971 is causing a negative impact on another internal process or system, and should be reversed to discontinue the negative impact. For example, a programming issue.
FALSE	RESERVED
OTHER	The reason for the 971 reversal does not meet any of the reason descriptions above.

5. The following tables describe the TC 972 AC 501 reason codes by BOD/Function and Program. Refer to Exhibit 25.23.2-1, *Acronyms and Definitions*, for definitions of the Program Name codes.

Note: Do not attempt to use Tax Administration Source Codes not listed for your BOD/Function.

6. Appeals is profiled to use the following codes to reverse a TC 971 AC 501:

BOD Name	Program Name	TC 972 AC 501 Tax Administration Source Code
AP	AP	TPRQ, IRSERR, IRSADM, FALSE, and OTHER

7. Criminal Investigation is profiled to use the following codes to reverse a TC 971 AC 501:

BOD Name	Program Name	TC 972 AC 501 Tax Administration Source Code
CI	FO	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
CI	RC	TPRQ, IRSERR, IRSADM, FALSE, and OTHER

8. Large Business & International (LB&I) is profiled to use the following codes to reverse a TC 971 AC 501:

BOD Name	Program Name	TC 972 AC 501 Tax Administration Source Code
LBI	LBI	TPRQ, IRSERR, IRSADM, FALSE, and OTHER

9. IT is profiled to use the following codes to reverse a TC 971 AC 501:

Exhibit 25.23.2-3 (Cont. 2) (10-01-2018)

#

BOD Name	Program Name	TC 972 AC 501 Tax Administration Source Code
MIT5	CSIRC	TPRQ, IRSERR, IRSADM, FALSE, and OTHER

10. The IPSO is profiled to use the following codes to reverse a TC 971 AC 501:

BOD Name	Program Name	TC 972 AC 501 Tax Administration Source Code
PPDS	CONGINQ	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
PPDS	OPIP	TPRQ, IRSERR, IRSADM, FALSE, and OTHER

11. Small Business Self Employed (SBSE) is profiled to use the following codes to reverse a TC 971 AC 501:

BOD Name	Program Name	TC 972 AC 501 Tax Administration Source Code
SBSE	CFBALDUE	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
SBSE	CFDELRET	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
SBSE	FLDEXAM	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
SBSE	FLDADV	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
SBSE	FLDINSLV	TPRQ, IRSERR, IRSADM, FALSE, and OTHER

12. Taxpayer Advocate Service (TAS) is profiled to use the following codes to reverse a TC 971 AC 501:

BOD Name	Program Name	TC 972 AC 501 Tax Administration Source Code
TAS	TAS	TPRQ, IRSERR, IRSADM, FALSE, and OTHER

13. Taxpayer Services (TS) is profiled to use the following codes to reverse a TC 971 AC 501:

Exhibit 25.23.2-3 (Cont. 3) (10-01-2018)

#

BOD Name	Program Name	TC 972 AC 501 Tax Administration Source Code
WI	FA	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
WI	AM	TPRQ
WI	IP	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
WI	ITVAA	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
WI	ITVAC	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
WI	PRP	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
WI	PREREF	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
WI	RICS	TPRQ, IRSERR, IRSADM, FALSE, and OTHER

Identity Protection and Victim Assistance - General Case Processing 25.23.2

page 115

Exhibit 25.23.2-4 (09-06-2023)

IMF Only TC 971 AC 504

TC 971 AC 504 is displayed on IDRS command code ENMOD and consists of the following data elements:

TRANS DATE	SECONDARY DATE	MISC	REMARKS
Input date of TC 971 AC 504	Date identity theft occurred (Use the table below to determine the secondary date. Caution: See IRM 25.23.2.3.8.1, <i>Command code REQ77 Secondary Date and Old Case Year Issue</i> , for Secondary Date limitations and other necessary input. For more information on CC REQ77 see IRM 2.4.19, <i>Command Codes REQ77, FRM77 and FRM7A</i> , or the <i>IDRS Command Code Job Aid</i> .	Taxpayer impact. (Use the table below to determine the correct MISC code based on the impact to the taxpayer.)	Comments

Exception: If making a determination of Income Related IDT, the secondary date will be the tax year impacted in the format of 1231YYYY. See IRM 25.23.2.8.1.1, *TC 971 AC 504 with Miscellaneous Field Codes ACCT, ACCT-M, BOTH, BOTH-M, EMPL, EMPL-M, ICMCCA, NKI or NKI-M* for more information.

Reminder: If a TC 971 AC 504 is input as a closing code, then a reversal of the existing TC 971 AC 522 is not required.

Secondary Date Field is required on input of all TC 971 AC 504. Some taxpayers provide an incomplete incident date or no incident date at all. In these situations, follow in order as outlined below:

Note: Use the tax year of the incident in the Secondary Date Field if applying the AC 504 using SPCL1, SPCL2, RPM1, RPM2, RPM3 AND RPM4, or EAFAIL.

If	THEN
1. Form 14039 specifies an incident date that is complete Note: A complete date is one that includes, Month, Day and Year.	Use the date provided on Form 14039. Example: The taxpayer indicates the ID theft occurred on October 15, 2019; the secondary date will reflect 10152019.

Exhibit 25.23.2-4 (Cont. 1) (09-06-2023)
IMF Only TC 971 AC 504

If	THEN
2. Additional documentation attached specifies an incident date that is complete. Note: A complete date is one that includes, Month, Day and Year.	Use the completion date provided in the additional documentation. Example: The Form 14039 does not include a complete incident date, but a copy of the police report is included with the claim. The report indicates the identity theft occurred on March 10, 2020; the secondary date will reflect 03102020
3. Form 14039 indicates an incident date of only a month and year	Use the first day of the month provided by the taxpayer on Form 14039. Example: The taxpayer indicates the ID theft occurred in October 2019; the secondary date will reflect 10012019.
4. Form 14039 lists a tax year (or multiple years), but there is no indication of tax related identity theft and no specific incident date is provided in the explanation.	Use the earliest tax period listed on Form 14039. Example: The Form 14039 indicates impact to 2017, 2018 and 2019; the secondary date will reflect 12312017. Note: If multiple tax years are listed on the Form 14039, use the earliest tax year. See IRM 25.23.2.3.8.1, <i>Command Code REQ77 Secondary Date and Old Case Year Issue</i> , for Secondary Date limitations.
5. Form 14039 does not include an incident date.	Use the Received date on the Form 14039. Example: The Form 14039 was received April 29, 2019; secondary date will reflect 04292019.

Input of Action Code 504 for non-tax related identity theft purposes is limited and reserved for use by IDTVA in TS Accounts Management. The following Miscellaneous Field Codes are used for non-tax-related identity theft while inputting TC 971 AC 504 using CC REQ77 or the REQ77 IAT tool:

		#
		#
		#
		#
		#

Identity Protection and Victim Assistance - General Case Processing 25.23.2

page 117

Exhibit 25.23.2-4 (Cont. 2) (09-06-2023)

IMF Only TC 971 AC 504

		#
		#
		#
		#
		#
		#
		#

Note: The MISC codes contain a “M” next to them to identify cases requiring a manual 4402C instead of a systemic notice (CP01C (English) and CP701C (Spanish)). The notice will be issued once the TC 971 AC 504 and original MISC codes posts to the TP’s account. Refer to IRM 25.23.3.2.3, *Self-Identified - Non-Tax-Related Identity Theft – IDT4 Overview*, for circumstances that would require the issuance of a manual 4402C letter.

Caution: Taxpayer accounts disabled from the Secure Access application who filed Form 14039, will be flagged with TC 971 AC 506 WI AM OTHER. You can identify these taxpayers by reviewing CC ENMOD or IMFOLE for an unreversed TC 971 AC 527 WI BREACH DSABLD

The following Miscellaneous Field Codes are used for BMF and RPM inventory programs using CC REQ77 or the REQ77 IAT tool:

Caution: CC REQ77 will accept an XREF EIN when an individual TP is reporting BMF Identity Theft.

Impact to Taxpayer		
Miscellaneous Field Codes	Description	
		#
		#
		#
		#
		#
		#
		#
		#
		#
		#
		#

Exhibit 25.23.2-4 (Cont. 3) (09-06-2023)
IMF Only TC 971 AC 504

#####

Identity Protection and Victim Assistance - General Case Processing 25.23.2

page 119

Exhibit 25.23.2-5 (09-08-2015)

IMF Only TC 972 AC 504 — Reversal of TC 971 AC 504

The miscellaneous field for TC 972 AC 504 reflects the reason for the reversal of TC 971 AC 504. See the TC 972 AC 504 Miscellaneous Field chart below for the reasons and values for the MISC field.

Reason	Description	Value
Taxpayer Request	The taxpayer requests the 971 be reversed.	TPRQ
Keying or Internal Error	The 971 was due to a typographical mistake or other internal mistake.	IRSERR
Internally Identified Negative Impact	The 971 is causing a negative impact on another internal process or system, and should be reversed to discontinue the negative impact. For example, a programming issue.	IRSADM
False Identity Theft Claim	RESERVED	FALSE
Other	The reason for the 971 reversal does not meet any of the reason descriptions above.	OTHER

Exhibit 25.23.2-6 (09-12-2019)
IMF Only TC 971 AC 505 — IRS Data Breaches

Important: Input of Action Code 505 is limited and reserved for use by PGLD personnel.

TC 971 AC 505 is displayed on IDRS command code ENMOD and consists of the following data elements:

TRANS-DT	SECONDARY-DT	MISC
TC 971 AC 505 input date	Date the data breach occurred.	Incident Reference Code number assigned to the data loss case. Usually, this number begins with the literal “IR” and is followed by 11 numeric digits. For example: IR20080211034

Exhibit 25.23.2-7 (09-08-2015)**IMF Only TC 972 AC 505 — Reversal of TC 971 AC 505**

The miscellaneous field for TC 972 AC 505 reflects the reason for the reversal of TC 971 AC 505. See the following chart for reasons and values for the MISC field:

Reason	Description	Value
Keying or Internal Error	The 971 was due to a typographical mistake or another internal mistake.	IRSERR
Internally Identified Negative Impact	The 971 is causing a negative impact on another internal process or system, and should be reversed to discontinue the negative impact. For example, a programming issue.	IRSADM
Other	The reason for the 971 reversal does not meet any of the above reason descriptions.	OTHER

Exhibit 25.23.2-8 (10-01-2018)**IMF Only TC 971 AC 506 — IRS Determined Tax-Related Identity Theft Case Closure**

The exhibit below demonstrates how SP inputs a TC 971 AC 506 when resolving IRS-identified identity theft issue involving an unpostable.

```

FRM77 XXX-XX-XXXX    MFT>00    TX-PRD> 000000    PLN-NUM>    NM-CTRL>
XXXXXX
TC>971    TRANS-REGISTER-IND>    PSTNG-DLAY-CD>
EXTENSION-DT>    TC93X-EMP-CD>    TRANS-DT>
CLOSING-CD>    RESP-UNIT/JURISDICTION-CD>    TC148-CD>
DLN-CD>    BL-LOC-CD>    LAST-RET-AMT-CD>    TC480-SC-CD>
CYCLE>    APP-OFF-CD>    CSED-CD>    BOD-CD>    BOD-CLIENT-CD>
SEQ-NUM>    REVERSAL-DLN>    SECONDARY-DT>12312009
CAF-CD>    TC971/151-CD> 506    TC550DEFINER-CD>    FEMA-NUM>
ULC>    FREEZE-RELEASE-AMT>    ABA-NUM>
TC46X-GRP-CD>    TC583-DEFINER-CD>
XREF-TIN>    XREF-NM-CTRL>
XREF-TIN-PRD>    XREF-PLN-NUM>    XREF-MFT>    MISC>WI SP UPC147
CORR-DT-IND>    REFILE-LIEN-*IND>    2032-IND>
REMARKS: Identity Theft

```

Input instructions for TC 971 AC 506 are as follows:

1. Obtain the following information:
 - Entity - SSN;
 - Business Operating Division (BOD)/Function (See Exhibit 25.23.2-1, *Acronyms and Definitions*;
 - Program Name (See Exhibit 25.23.2-1, *Acronyms and Definitions*);
 - Tax Administration Source (See Exhibit 25.23.2-1, *Acronyms and Definitions*); and
 - Tax Year affected by identity theft.

Note: The tax year affected by the identity theft **cannot** be the current year. For example, the taxpayer gives you a valid claim during the current year for a 2013 tax year issue. Input TC 971 AC 506 on tax year 2013 only.

2. The tables provided below display the available Tax Administration Source Codes by BOD/Function (Program). Do not attempt to use Tax Administration Source Codes not listed for your BOD/Function (Program).
3. Navigate to CC FRM77
 - Sign into IDRS;
 - Enter ENMOD (SSN), then press ENTER;
 - Enter CC REQ77;
 - FRM77 is displayed for the selected SSN.
4. Enter the TC 971 AC 506
 - Enter the TC with 971;
 - TRANS-DT is auto populated with the current date;
 - Enter SECONDARY-DT (enter the tax year affected by the identity theft incident in the format MM-DD-YYYY);

Caution: See Exhibit 25.23.2-2, *IMF Only TC 971 AC 501 — Taxpayer Initiated Identity Theft Case Closure (Tax-Related) - TC 971 AC 501*, for Secondary Date limitations and other necessary input. For more information on CC REQ77 see IRM 2.4.19, *Command Codes REQ77, FRM77 and FRM7A*, or the *IDRS Command Code Job Aid*.

Identity Protection and Victim Assistance - General Case Processing 25.23.2

page 123

Exhibit 25.23.2-8 (Cont. 1) (10-01-2018)

IMF Only TC 971 AC 506 — IRS Determined Tax-Related Identity Theft Case Closure

- Enter MISC (enter your specific BOD/Function, Program Name, and Tax Administration Source; see the BOD/Function tables below); and
- After REMARKS, enter "IDENTITY THEFT".

Note: See the illustration above, demonstrating how SP inputs a TC 971 AC 506 after resolving an un-postable 147 RC1 case.

5. Tax Administration Source Codes for use with TC 971 AC 506 - IRS Determined Case Closure

Note: Taxpayers affected by Get Transcript incident who filed Form 14039, will be flagged with TC 971 AC 506 WI AM OTHER. You can identify these taxpayers by reviewing CC ENMOD for a TC 971 AC 505 IR20150521512, TC 971 AC 505 IR20150521555, or TC 971 AC 505 IR20150521556.

TC 971 AC 506 Tax Administration Codes	Definition of Tax Administration Source Code
INCOME	Identity theft identified and substantiated due to an underreporting of income
MULTFL	Identity theft identified and substantiated due to two or more tax returns filed for one taxpayer
INCMUL	Identity theft identified and substantiated due to both underreporting of income and multiple filings
OTHER	Identity theft which cannot be identified as related to any existing Tax Administration Source types or when TP files F 14039 in response to EPSS disabled account to put TP in CP01A population.
OTHER1	Used exclusively by RICs to identify an SSN where there is either: <ul style="list-style-type: none">• Used to mark accounts that have been identified as having previous tax-related identity theft situation, but have a good taxpayer involved with a verified good address of record. These markers will receive the IP PIN notice
OTHER2	FS 2015- Used Exclusively by RICS to issue the CP01F IP PIN OPT-In Notice for the TC 971 504 EAFail population, as well as TINS identified by CI to be compromised by a data breach when the posted return was verified as Non-IDT based on IRP and the zip code on the return matches the current year IRP address.
LIST1	Used exclusively by RICs to accounts referred by Criminal Investigation (CI) involving data breach lists. Also includes high risk (e.g., PII, hacked preparer) and imminent lists such as Traffic Stops, Search Warrants, and Informant Leads, with no returns filed.

Exhibit 25.23.2-8 (Cont. 2) (10-01-2018)

IMF Only TC 971 AC 506 — IRS Determined Tax-Related Identity Theft Case Closure

TC 971 AC 506 Tax Administration Codes	Definition of Tax Administration Source Code
NOFR	Identity theft identified by the filing of a false return in order to obtain a refund and the good taxpayer has no filing requirement
DECD	Deceased taxpayer
PRISNR	Incarcerated Taxpayer
NKI and NKI-M	Used by RICS Pre-Refund for CI cases with no known impact on taxpayer account
IDT	Used by RICS Pre-Refund for CI Cases where a bad return was filed under the taxpayer's SSN
DDb	Used by RICS Pre-Refund for cases selected by DDb filter and identified as an Identity Theft return
SSA	Used by RICS Pre-Refund for cases identified by SSA filters, but are confirmed Identity Theft cases
OMM	Previously used by RICS Pre-Refund for cases selected by DDb Filter that are OMM Cases.
UPCMUL	Input on true SSN owner's account when a non-legitimate unpostable return with UPC147 RC 1 has been filed using the taxpayer's SSN as identified and determined by SP
UPC147	Input on the identified IRSN corresponding to the non-legitimate unpostable return with UPC147 RC 1 as identified and determined by SP
OMMGB	Valid return filed by the legitimate taxpayer who was previously identified as OMM
ERC027	Primary Taxpayer under 14 years old

6. Do not attempt to use a Tax Administration Source Code that your BOD/Program (Function) is not profiled to use. The following table identifies the BOD/Programs and applicable Tax Administration Source Codes. Refer to Exhibit 25.23.2-1, *Acronyms and Definitions*, for definitions of the Program Name codes.
7. **The following BODS are not profiled to use TC 971 AC 506: Appeals, TAS, LB&I, and IT. Important: Input of Action Code 506 is limited and reserved for use by designated functions. The BOD Tables below illustrate only those Functions/Programs authorized to use TC 971 AC 506.**
Note: At present, TS Field Assistance (FA) is not profiled for AC 506. Until further notice when resolving IRS determined cases, TS FA will use the following:
BOD: WI
Program: AM
Tax Administration Source Codes: INCOME, and OTHER.
8. Criminal Investigation is profiled to use TC 971 AC 506 as follows:

Identity Protection and Victim Assistance - General Case Processing 25.23.2

page 125

Exhibit 25.23.2-8 (Cont. 3) (10-01-2018)

IMF Only TC 971 AC 506 — IRS Determined Tax-Related Identity Theft Case Closure

BOD Name	Program Name	TC 971 AC 506 Tax Administration Source Code
CI	PHSH	<i>Field intentionally left blank</i>
CI	RFND	<i>Field intentionally left blank</i>
CI	OTHER	<i>Field intentionally left blank</i>
CI	RC	PRISNR
CI	RC	DECD

9. SBSE is profiled to use the following codes:

BOD Name	Program Name	TC 971 AC 506 Tax Administration Source Code
SBSE	CFBALDUE	INCOME, MULTFL, INCMUL, OTHER, NOFR, PRISNR, and DECD
SBSE	CFDELRET	INCOME, MULTFL, INCMUL, OTHER, NOFR, PRISNR, and DECD
SBSE	FLDEXAM	INCOME, MULTFL, INCMUL, OTHER, NOFR, PRISNR, and DECD
SBSE	FLDADV	INCOME, MULTFL, INCMUL, OTHER, NOFR, PRISNR, and DECD
SBSE	FLDINSLV	INCOME, MULTFL, INCMUL, OTHER, NOFR, PRISNR, and DECD

10. Taxpayer Services (TS) is profiled with the following codes:

BOD Name	Program Name	TC 971 AC 506 Tax Administration Source Code
WI	AM	OTHER
WI	IP	DECD, INCMUL, INCOME, MULTFL, NOFR, OTHER, PRISNR, MISC1, MISC2, MISC3, MISC4 and MISC5
WI	ITVAA	INCMUL, INCOME, MULTFL, NOFR, OTHER and PRISNR

Exhibit 25.23.2-8 (Cont. 4) (10-01-2018)**IMF Only TC 971 AC 506 — IRS Determined Tax-Related Identity Theft Case Closure**

BOD Name	Program Name	TC 971 AC 506 Tax Administration Source Code
WI	ITVAC	INCMUL, INCOME, MULTFL, NOFR, OTHER and PRISNR
WI	IVO	DECD, OTHER, PRISNR and RFND
WI	PRP	DDB, DECD, IDT, INCMUL, INCOME, LIST1, LIST2, LIST3, LIST4, LIST5, LIST6, MULTFL, NKI, NOFR, OMM, OTHER, OTHER1, OTHER2, OTHER3, OTHER4, OTHER5, PRISNR and SSA
WI	RICS	INCOME, MULTFL, INCMUL, OTHER, NOFR, PRISNR,
WI	SP	INCOME, INCMUL, MULTFL, OTHER, NOFR, DECD, PRISNR, EC029, UPC147, and UPCMUL

Exhibit 25.23.2-9 (04-16-2021)**IMF Only TC 972 AC 506 Tax-Related, Reversal of Identity Theft Case Closure, IRS Identified**

The illustration below demonstrates how Accounts Management reverses a TC 971 AC 506 using a TC 972 AC 506.

#

Input instructions for TC 972 AC 506 are as follows:

1. Obtain the following information:
 - Entity - SSN;
 - BOD/Function (See Exhibit 25.23.2-1, *Acronyms and Definitions*);
 - Program Name (See Exhibit 25.23.2-1, *Acronyms and Definitions*);
 - Tax Year of the TC 971 AC 506 being reversed; and

Note: The tax year must match the tax year of the TC 971 AC 506 that is being reversed.

 - Transaction date of the TC 971 AC 506 being reversed.
2. Navigate to CC FRM77
 - Sign into IDRS;
 - Enter ENMOD SSN, then press ENTER;
 - Enter CC REQ77;
 - FRM77 is displayed for the selected SSN.
3. Enter the TC 972 AC 506

Exception: If the year in question being reversed is older than the current calendar year minus 7 years, CC REQ77 will not accept the year. See IRM 25.23.2.3.8.1, *Command Code REQ77 Secondary Date and Old Case Year Issue* for more information.

 - Enter the TC with 972;
 - Enter TRANS-DT (enter the transaction date of the TC 971 AC 506 being reversed);
 - Enter SECONDARY-DT (enter the tax year of the TC 971 AC 506 being reversed in the MMDDYYYY format);
 - Enter MISC (Modify the Reason Code field with the reason for the reversal). Select the Reason code that reflects the reason for the reversal from the options below; and
 - Enter REMARKS (enter your remarks).

Exhibit 25.23.2-9 (Cont. 1) (04-16-2021)**IMF Only TC 972 AC 506 Tax-Related, Reversal of Identity Theft Case Closure, IRS Identified**

Note: Do not attempt to use Tax Administration Source Codes not listed for your BOD/Function.

4. Tax Administration Source Code is entered into the Miscellaneous field and displays the reason for the reversal. See TC 972 AC 506 Miscellaneous Field chart below for reasons and values for the MISC field:

TC 972 AC 506 Tax Administration Source Code	Definition
TPRQ	The taxpayer requests the 971 be reversed.
IRSERR	The 971 was due to a typographical mistake or another internal mistake.
IRSADM	The 971 is causing a negative impact on another internal process or system, and should be reversed to discontinue the negative impact. For example, a programming issue.
FALSE	RESERVED
OTHER	The reason for the 971 reversal does not meet any of the reason descriptions above.

5. **The following BODS are not profiled to use TC 972 AC 506: Appeals, TAS, LB&I, and IT.**
 6. The following tables describe the TC 972 AC 506 reason codes by BOD/Function and Program. Refer to Exhibit 25.23.2-1, *Acronyms and Definitions*, for definitions of the Program Name codes.

Note: Do not attempt to use Tax Administration Source Codes not listed for your BOD/Function.

7. Criminal Investigation is profiled to use TC 972 AC 506 as follows:

BOD Name	Program Name	TC 972 AC 506 Tax Administration Source Code
CI	OTHER	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
CI	PHSH	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
CI	RC	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
CI	RFND	TPRQ, IRSERR, IRSADM, FALSE, and OTHER

8. Operations Support (OS) is profiled to use TC 972 AC 506 as follows:

BOD Name	Program Name	TC 972 AC 506 Tax Administration Source Code
OS	PIPDS	TPRQ, IRSERR, IRSADM, FALSE, and OTHER

9. Small Business Self Employed (SBSE) is profiled to use TC 972 AC 506 as follows:

Exhibit 25.23.2-9 (Cont. 2) (04-16-2021)

IMF Only TC 972 AC 506 Tax-Related, Reversal of Identity Theft Case Closure, IRS Identified

BOD Name	Program Name	TC 972 AC 506 Tax Administration Source Code
SBSE	CFBALDUE	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
SBSE	CFDELRET	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
SBSE	FLDEXAM	TPRQ, IRSERR, IRSADM, OTHER, and FALSE
SBSE	FLDADV	TPRQ, IRSERR, IRSADM, OTHER, and FALSE
SBSE	FLDINSLV	TPRQ, IRSERR, IRSADM, OTHER, and FALSE

10. Taxpayer Services (TS) is profiled to use TC 972 AC 506 as follows:

BOD Name	Program Name	TC 972 AC 506 Tax Administration Source Code
WI	IP	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
WI	ITVAA Note: Must be input as ITVAA. This was a clerical error in programming.	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
WI	IVTAC Note: Must be input as IVTAC. This was a clerical error in programming.	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
WI	AM	TPRQ
WI	IVO	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
WI	RICS	TPRQ, IRSERR, IRSADM, FALSE, and OTHER
WI	SP	TPRQ, IRSERR, IRSADM, and FALSE

Exhibit 25.23.2-10 (11-01-2021)**IMF Only TC 971 AC 522 Tax-Related Identity Theft, Case Status (Initial Claim/Suspicion)**

The exhibit demonstrates how AUR inputs a TC 971 AC 522 when the taxpayer initially asserts identity theft.

Note: If the allegation or suspicion of IDT is for an Economic Impact Payment (EIP), check the TC 971 AC 199 on IMFOLE to see the source of the EIP. If the source is a 2018 return, input 2018 as the tax year affected by IDT. If the source is something other than a 2018 return, input 2019 as the tax year affected.

```

FRM77 XXX-XX-XXXX    MFT>00    TX-PRD> 000000    PLN-NUM>    NM-CTRL> XXXXXX
TC>971    TRANS-REGISTER-IND> PSTNG-DLAY-CD>
EXTENSION-DT>    TC93X-EMP-CD>    TRANS-DT>
CLOSING-CD>    RESP-UNIT/JURISDICTION-CD>    TC148-CD>
DLN-CD>    BL-LOC-CD>    LAST-RET-AMT-CD>    TC480-SC-CD>
CYCLE>    APP-OFF-CD>    CSED-CD>    BOD-CD>    BOD-CLIENT-CD>
SEQ-NUM>    REVERSAL-DLN>    SECONDARY-DT>12312009
CAF-CD>    TC971/151-CD> 522    TC550DEFINER-CD>    FEMA-NUM>
ULC>    FREEZE-RELEASE-AMT>    ABA-NUM>
TC46X-GRP-CD>    TC583-DEFINER-CD>
XREF-TIN>    XREF-NM-CTRL>
XREF-TIN-PRD>    XREF-PLN-NUM>    XREF-MFT>    MISC>WI AUR PNDCLM
CORR-DT-IND>    REFILE-LIEN-*IND>    2032-IND>
REMARKS: Identity Theft

```

Input instructions for TC 971 AC 522 are as follows:

1. Obtain the following information:

- Entity - SSN;
- BOD/Function (See Exhibit 25.23.2-1, *Acronyms and Definitions*);
- Program Name (See Exhibit 25.23.2-1, *Acronyms and Definitions*);
- Tax Administration Source (See Exhibit 25.23.2-1, *Acronyms and Definitions*); and
- Tax Year affected by identity theft.

Note: The tax year affected by the identity theft **cannot** be the current year. For example, the taxpayer submits a valid claim during the current year, for a 2014 tax year issue. Input TC 971 AC 522 on tax year 2014 only and not on the current year.

Caution: The Secondary Date field on CC REQ77 is limited to the current calendar year and 7 prior years. The secondary date field will not allow the input of any date outside that range. See IRM 25.23.2.3.8.1, *Command Code REQ77 Secondary Date and Old Case Year Issue* for more information.

2. The tables provided below display the available Tax Administration Source Codes by BOD/Function (Program). Do not attempt to use Tax Administration Source Codes not listed for your BOD/Function (Program).

Exception: See "NOTE" under Charts below for BOD/Function for Tax Administration Codes: UNWORK & IRSID.

3. Navigate to CC FRM77

- Sign into IDRS;
- Enter ENMOD SSN, then press ENTER;
- Enter CC REQ77;
- FRM77 is displayed for the selected SSN.

Exhibit 25.23.2-10 (Cont. 1) (11-01-2021)

IMF Only TC 971 AC 522 Tax-Related Identity Theft, Case Status (Initial Claim/Suspicion)

4. Enter the TC 971 AC 522
 - TC> Enter the TC with 971;
 - TC 971/151-CD> Enter 522
 - TRANS-DT is auto-populated with the current date;
 - Enter SECONDARY-DT (enter the tax year affected by the identity theft incident in the format MMDDYYYY);

Note: If the taxpayer is reporting more than one year affected by identity theft, the Secondary-DT field will reflect the tax year affected by identity theft.

 - Enter MISC (enter your specific BOD/Function, Program Name, and Tax Administration Source) see Exhibit 25.23.2-1, *Acronyms and Definitions*, and
 - After REMARKS, enter "IDENTITY THEFT".
5. Tax Administration Source codes for use with TC 971 AC 522 – Identity Theft Account Status:

TC 971 AC 522 Tax Administration Source Code	Definition
PNDCLM	The taxpayer has made an allegation of identity theft by telephone, has filed a return with a claim attached or has sent a reply to a Compliance function alleging identity theft without a Form 14039 or police report.
IRSID	During the normal course of business, the IRS suspects identity theft may have occurred, and the case is not yet resolved.
NODCRQ	Beginning in 2015, used in conjunction with BOD PPDS and Program OPIP (TC 971 AC 522 PPDS OPIP NODCRQ) to identify/track on-line accounts and EPSS accounts disabled due to identity theft. Prior to 2015, NODCRQ was applied when the taxpayer claimed identity theft and there was a posted TC 971 AC 501/ 506.
UNWORK	An Identity Theft Claim (see Exhibit 25.23.2-1, <i>Acronyms and Definitions</i>) has been received but has not been resolved yet. Note: Campus Compliance functions will only refer cases with Form 14039 or a police report, use this Tax Source only if one of them have been received.

6. The tables provided below display the available Tax Administration Source Codes by BOD/Function and Program. **Do not attempt to use Tax Administration Source Codes not listed for your BOD/Function.**
7. **Appeals (AP)** is profiled to use the following codes for TC 971 AC 522:

Exhibit 25.23.2-10 (Cont. 2) (11-01-2021)

IMF Only TC 971 AC 522 Tax-Related Identity Theft, Case Status (Initial Claim/Suspicion)

BOD Name	Program Name	TC 971 AC 522 Tax Administration Source Code
AP	AP	ALTRD, INCMUL, INCOME, IRSID, MULTFL, NODCRQ, NOFR, OTHER, PNDCLM and UNWORK

8. **Criminal Investigation (CI)** is profiled to use the following codes for TC 971 AC 522:

BOD Name	Program Name	TC 971 AC 522 Tax Administration Source Code
CI	FO	ALTRD, BOTH, INCMUL, INCOME, MULTFL, NOFR and OTHER
CI	RC	ALTRD, DECD, INCMUL, IRSID, INCOME, MULTFL, NOFR, UNWORK and OTHER

9. **Large Business & International (LB&I)** is profiled to use the following codes for TC 971 AC 522:

BOD Name	Program Name	TC 971 AC 522 Tax Administration Source Code
LBI	LBI	INCMUL, IRSID, INCOME, MULTFL, NODCRQ, NOFR, PNDCLM, UNWORK and OTHER

10. **IT** is profiled to use the following codes for TC 971 AC 522:

BOD Name	Program Name	TC 971 AC 522 Tax Administration Source Code
MIT	CSIRC	ALTRD, NOFR and OTHER

11. **Operations Support (OS)** is profiled to use the following codes for TC 971 AC 522:

BOD Name	Program Name	TC 971 AC 522 Tax Administration Source Code
OS	PHSH	NODCRQ, IRSID and UNWORK

12. **Small Business Self Employed (SBSE)** is profiled to use the following codes for TC 971 AC 522:

Identity Protection and Victim Assistance - General Case Processing 25.23.2

page 133

Exhibit 25.23.2-10 (Cont. 3) (11-01-2021)

IMF Only TC 971 AC 522 Tax-Related Identity Theft, Case Status (Initial Claim/Suspicion)

BOD Name	Program Name	TC 971 AC 522 Tax Administration Source Code
SBSE	ACS	PNDCLM Note: for UNWORK and IRSID, see NOTE below
SBSE	ASFR	PNDCLM Note: for UNWORK and IRSID, see NOTE below
SBSE	AUR	PNDCLM Note: for UNWORK and IRSID, see NOTE below
SBSE	CFBALDUE	INCMUL, IRSID, INCOME, MULTFL, NOFR, PNDCLM, UNWORK and OTHER
SBSE	CFDELRET	ALTRD, INCMUL, IRSID, INCOME, MULTFL, NODCRQ, NOFR, PNDCLM, UNWORK and OTHER
SBSE	CORR	PNDCLM Note: for UNWORK and IRSID, see NOTE below
SBSE	CSCO	PNDCLM Note: for UNWORK and IRSID, see NOTE below
SBSE	FLDADV	INCMUL, IRSID, INCOME, MULTFL, NODCRQ, NOFR, PNDCLM, UNWORK and OTHER
SBSE	FLDEXAM	ALTRD, INCMUL, IRSID, INCOME, MULTFL, NODCRQ, NOFR, PNDCLM, UNWORK and OTHER
SBSE	FLDINSLV	ALTRD, INCMUL, IRSID, INCOME, MULTFL, NODCRQ, NOFR, PNDCLM, UNWORK and OTHER

Exhibit 25.23.2-10 (Cont. 4) (11-01-2021)

IMF Only TC 971 AC 522 Tax-Related Identity Theft, Case Status (Initial Claim/Suspicion)

BOD Name	Program Name	TC 971 AC 522 Tax Administration Source Code
SBSE	TDI	PNDCLM Note: for UNWORK and IRSID, see NOTE below
SBSE	TEFRA	PNDCLM Note: for UNWORK and IRSID, see NOTE below

Note: SBSE employees will need to use either “WI ITVAA UNWORK” or “WI ITVAA IRSID” on any non-compliance related issue and use either “WI ITVAC UNWORK” or “WI ITVAC IRSID” on any compliance related issue when inputting UNWORK or IRSID Tax Source Administration Codes.

13. **Taxpayer Advocate Service (TAS)** is profiled to use the following codes for TC 971 AC 522:

BOD Name	Program Name	TC 971 AC 522 Tax Administration Source Code
TAS	CA	PNDCLM, IRSID, and UNWORK

14. **Taxpayer Services (TS)** is profiled to use the following codes for TC 971 AC 522:

BOD Name	Program Name	TC 971 AC 522 Tax Administration Source Code
WI	ACS	PNDCLM Note: for UNWORK and IRSID, see NOTE below
WI	AM	PNDCLM Note: for UNWORK and IRSID, see NOTE below
WI	ASFR	PNDCLM Note: for UNWORK and IRSID, see NOTE below
WI	AUR	PNDCLM Note: for UNWORK and IRSID, see NOTE below

Identity Protection and Victim Assistance - General Case Processing 25.23.2

page 135

Exhibit 25.23.2-10 (Cont. 5) (11-01-2021)

IMF Only TC 971 AC 522 Tax-Related Identity Theft, Case Status (Initial Claim/Suspicion)

BOD Name	Program Name	TC 971 AC 522 Tax Administration Source Code
WI	CSCO	PNDCLM Note: for UNWORK and IRSID, see NOTE below
WI	EXAM	PNDCLM Note: for UNWORK and IRSID, see NOTE below
WI	FA	ALTRD, INCMUL, IRSID, INCOME, ITIN, MULTFL, NODCRQ, NOFR, PNDCLM, UNWORK and OTHER
WI	ITVAA	INCMUL, IRSID, INCOME, ITIN, MULTFL, NODCRQ, NOFR, PNDCLM, UNWORK and OTHER
WI	ITVAC	INCMUL, IRSID, INCOME, ITIN, MULTFL, NODCRQ, NOFR, PNDCLM, UNWORK and OTHER
WI	IVO	DECD, INCMUL, INCOME, IRSID, MILTFL, NODCRQ, OTHER, PNDCLM, PRISNR AND UNWORK
WI	PREREF	ALTRD, DECD, INCMUL, IRSID, INCOME, MULTFL, NODCRQ, NOFR, PNDCLM, PRISNR, UNWORK and OTHER
WI	RICS	DECD, INCMUL, IRSID, INCOME, MULTFL, NODCRQ, NOFR, PNDCLM, UNWORK and OTHER
WI	SP	INCMUL, IRSID, INCOME, MULTFL, NODCRQ, PNDCLM, PRISNR, UNWORK and OTHER
WI	TDI	PNDCLM Note: for UNWORK and IRSID, see NOTE below

Exhibit 25.23.2-10 (Cont. 6) (11-01-2021)**IMF Only TC 971 AC 522 Tax-Related Identity Theft, Case Status (Initial Claim/Suspicion)**

BOD Name	Program Name	TC 971 AC 522 Tax Administration Source Code
WI	WHC	PNDCLM Note: for UNWORK and IRSID, see NOTE below

Note: TS employees will need to use either “WI ITVAA UNWORK” for UNWORK or “WI ITVAA IRSID” on any non-compliance related issue and use either “WI ITVAC UNWORK” for UNWORK or “WI ITVAC IRSID” on any compliance related issue when inputting UNWORK or IRSID Tax Source Administration Codes.

Exhibit 25.23.2-11 (10-01-2022)

IMF Only TC 972 AC 522 - Reversal of TC 971 AC 522

The exhibit demonstrates how IDTVA inputs a TC 971 AC 522 when no identity theft occurred.

Reminder: The TC 971 AC 504 is a closing code, just like the AC 501 and AC 506. All three identify the resolution of identity theft cases and close the TC 971 AC 522 claim. Do not manually reverse a TC 971 AC 522 previously closed with TC 971 AC 501/504/506. A TC 971 AC 522 that is unresolved may be reversed even if the secondary date is the same as a TC 971 AC 522 previously resolved by a TC 971 AC 501/504/506.

```

FRM77 XXX-XX-XXXX    MFT>00    TX-PRD> 000000    PLN-NUM>    NM-CTRL> XXXXXX
TC>972    TRANS-REGISTER-IND> PSTNG-DLAY-CD>
EXTENSION-DT>    TC93X-EMP-CD>    TRANS-DT> See Instructions Below
CLOSING-CD>    RESP-UNIT/JURISDICTION-CD>    TC148-CD>
DLN-CD>    BL-LOC-CD>    LAST-RET-AMT-CD>    TC480-SC-CD>
CYCLE>    APP-OFF-CD>    CSED-CD>    BOD-CD>    BOD-CLIENT-CD>
SEQ-NUM>    REVERSAL-DLN>    SECONDARY-DT>12312009
CAF-CD>    TC971/151-CD> 522    TC550DEFINER-CD>    FEMA-NUM>
ULC>    FREEZE-RELEASE-AMT>    ABA-NUM>
TC46X-GRP-CD>    TC583-DEFINER-CD>
XREF-TIN>    XREF-NM-CTRL>
XREF-TIN-PRD>    XREF-PLN-NUM>    XREF-MFT>    MISC>WI AUR NOIDT
CORR-DT-IND>    REFILE-LIEN-*IND>    2032-IND>
REMARKS: MIXED ENTITY, NOT IDENTITY THEFT
    
```

1. Obtain the following information:

- Entity - SSN;
- BOD/Function (See Exhibit 25.23.2-1, *Acronyms and Definitions*);
- Program Name (See Exhibit 25.23.2-1, *Acronyms and Definitions*);
- Tax Year of the TC 971 AC 522 being reversed; and

Note: The tax year must match the tax year of the TC 971 AC 522 that is being reversed.

- Transaction date of the TC 971 AC 522 being reversed.

2. Navigate to FRM77

- Sign into IDRS;
- Enter ENMOD SSN, then press ENTER;
- Enter CC REQ77;
- FRM77 is displayed for the selected SSN.

3. Enter the TC 972 AC 522

Caution: If the year in question being reversed is older than the current calendar year minus 7 years, CC REQ77 will not accept the year. See IRM 25.23.2.3.8.1, *Command Code REQ77 Secondary Date and Old Case Year Issue*, for more information.

- Enter the TC with 972;
- Enter TRANS-DT (enter the transaction date of the TC 971 AC 522 being reversed);

Caution: In rare instances the Transaction Date will be a future date. If it is a future date, suspend the case until that date before attempting to input the TC 972 AC 522. If the TC 971 AC 522 is pending, post delay the TC 972 AC 522 one week.

Exhibit 25.23.2-11 (Cont. 1) (10-01-2022)**IMF Only TC 972 AC 522 - Reversal of TC 971 AC 522**

- Enter SECONDARY-DT (enter the tax year of the TC 971 AC 522 being reversed in the MMDDYYYY format);
 - Enter MISC (Modify the Reason Code field with the reason for the reversal). Select the Reason code that reflects the reason for the reversal from the options below; and
 - Enter REMARKS (enter your remarks).
4. The following tables describe the TC 972 AC 522 Tax Administration Source Codes by BOD/Function and Program.

Note: Do not attempt to use Tax Administration Source Codes not listed for your BOD/Function.

Reason	Description	Tax Administration Source Code
Taxpayer claimed Identity Theft and Identity Theft has NOT occurred	In the course of resolving an identity theft issue, the employee assigned determines no identity theft occurred.	NOIDT
The taxpayer did not provide a valid claim or the requested additional information	This code is used to close a suspended case when the taxpayer fails to provide a valid claim or the requested additional information within the time specified by the employee assigned.	NORPLY
Taxpayer Request	The taxpayer requests the 971 be reversed.	TPRQ
Keying or Internal Error	The 971 was due to a typographical mistake or another internal mistake.	IRSERR
IRS determined possible identity theft (IRSID) and later determined no identity theft occurred	In the course of working the account, the employee assigned to the case subsequently found that no identity theft occurred	IRSERR
Internally Identified Negative Impact	The 971 is causing a negative impact on another internal process or system, and should be reversed to discontinue the negative impact. For example, a programming issue.	IRSADM
False Identity Theft Claim	RESERVED	FALSE
Other	The reason for the 971 reversal does not meet any of the above reason descriptions.	OTHER

The following tables describe the TC 972 AC 522 reason codes by BOD/Function and Program. Refer to Exhibit 25.23.2-1, *Acronyms and Definitions*, for definitions of the Program Name codes.

Note: Do not attempt to use Tax Administration Source Codes not listed for your BOD/Function.

Appeals is profiled to use the following codes to reverse a TC 971 AC 522:

Identity Protection and Victim Assistance - General Case Processing 25.23.2

page 139

Exhibit 25.23.2-11 (Cont. 2) (10-01-2022)

IMF Only TC 972 AC 522 - Reversal of TC 971 AC 522

BOD Name	Program Name	TC 972 AC 522 Tax Administration Source Code
AP	AP	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY, and OTHER

CI is profiled to use the following codes to reverse a TC 971 AC 522:

BOD Name	Program Name	TC 972 AC 522 Tax Administration Source Code
CI	FO	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY, and OTHER
CI	RC	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY, and OTHER

LB&I is profiled to use the following codes to reverse a TC 971 AC 522:

BOD Name	Program Name	TC 972 AC 522 Tax Administration Source Code
LBI	LBI	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, and OTHER

IT is profiled to use the following codes to reverse a TC 971 AC 522:

BOD Name	Program Name	TC 972 AC 522 Tax Administration Source Code
MIT	CSIRC	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY, and OTHER

Operations Support is profiled to use the following codes to reverse a TC 971 AC 522

BOD Name	Program Name	TC 972 AC 522 Tax Administration Source Code
OS	PHSH	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY, and OTHER

IPSO is profiled to use the following codes to reverse a TC 971 AC 522:

Exhibit 25.23.2-11 (Cont. 3) (10-01-2022)**IMF Only TC 972 AC 522 - Reversal of TC 971 AC 522**

BOD Name	Program Name	TC 972 AC 522 Tax Administration Source Code
PPDS	CONGINQ	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY, and OTHER
PPDS	OPIP	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY, and OTHER

SBSE is profiled to use the following codes to reverse a TC 971 AC 522:

BOD Name	Program Name	TC 972 AC 522 Tax Administration Source Code
SBSE	ACS	NORPLY
SBSE	ASFR	NORPLY
SBSE	AUR	NORPLY
SBSE	CFBALDUE	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY and OTHER
SBSE	CFDELRET	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY and OTHER
SBSE	CORR	NORPLY
SBSE	CSCO	NORPLY
SBSE	FLDADV	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY and OTHER
SBSE	FLDEXAM	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY RPM and OTHER
SBSE	FLDINSLV	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY and OTHER
SBSE	TDI	NORPLY
SBSE	TEFRA	NORPLY

TAS is profiled to use the following codes to reverse a TC 971 AC 522:

Identity Protection and Victim Assistance - General Case Processing 25.23.2

page 141

Exhibit 25.23.2-11 (Cont. 4) (10-01-2022)

IMF Only TC 972 AC 522 - Reversal of TC 971 AC 522

BOD Name	Program Name	TC 972 AC 522 Tax Administration Source Code
TAS	TAS	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY, and OTHER

Taxpayer Services (TS) is profiled to use the following codes to reverse a TC 971 AC 522:

BOD Name	Program Name	TC 972 AC 522 Tax Administration Source Code
WI	ACS	NORPLY
WI	AM	TPRQ
WI	ASFR	NORPLY
WI	AUR	NORPLY
WI	CSCO	NORPLY
WI	EXAM	NORPLY
WI	FA	ALTRD, TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY, and OTHER
WI	ITVAA	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY, and OTHER
WI	ITVAC	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY, and OTHER
WI	PREREF	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY, and OTHER
WI	RICS	TPRQ, IRSERR, IRSADM, FALSE, NOIDT, NORPLY, and OTHER
WI	SP	TPRQ, IRSERR, IRSADM, FALSE, OTHER, NOIDT and NORPLY
WI	TDI	NORPLY
WI	WHC	NORPLY

Exhibit 25.23.2-12 (10-13-2016)

TC 971 AC 523 – Reserved

Important: Input of Action Code 523 is limited and reserved for use by PGLD.

Exhibit 25.23.2-13 (10-13-2016)

#

The miscellaneous field for TC 972 AC 523 reflects the reason for the reversal of TC 971 AC 523.

Exhibit 25.23.2-14 (09-08-2015)**TC 971 AC 524 – Locking SSNs - Applies to IMF Accounts Only**

Important: Input of TC 971 AC 524 is limited and reserved for use by Identity Protection Strategy & Oversight (IPSO) and RICS.

The TC 971 AC 524 is displayed on IDRS command code ENMOD and consists of the following data elements:

TRANS-DT	SECONDARY-DT	MISC
Input date of TC 971 AC 524	Tax year of date of death	BOD, Function, and Program that input the TC 971 AC 524. (See the Miscellaneous Field table below.)

Below is a summary of the TC 971 AC 524 Miscellaneous Field elements:

Description	BOD / Function	Program Name	Tax Administration Source
Deceased Taxpayer	PPDS	OPIP	DECD
Deceased Taxpayer	WI	PREREF	DECD

Exhibit 25.23.2-15 (11-01-2021)

TC 972 AC 524 – Reversal of TC 971 AC 524

Important: Input of TC 972 AC 524 when there is a Date of Death is limited and reserved for use by the IPSO and Taxpayer Services (RICS TPP & Submission Processing Entity).

When there is **NO** date of death present CSRs may, after completing the required taxpayer authentication, reverse TC 971 AC 524.

The miscellaneous field for TC 972 AC 524 reflects the reason for the reversal of TC 971 AC 524. The transaction date of the TC 972 must match the original TC 971. See the TC 972 AC 524 Miscellaneous Field chart below for the reasons and values for the MISC field.

```

FRM77 XXX-XX-XXXX MFT>00 TX-PRD> 000000 PLN-NUM> NM-CTRL> XXXXXX
TC>972 TRANS-REGISTER-IND> PSTNG-DLAY-CD>
EXTENSION-DT> TC93X-EMP-CD> TRANS-DT> See Instructions Below
CLOSING-CD> RESP-UNIT/JURISDICTION-CD> TC148-CD>
DLN-CD> BL-LOC-CD> LAST-RET-AMT-CD> TC480-SC-CD>
CYCLE> APP-OFF-CD> CSED-CD> BOD-CD> BOD-CLIENT-CD>
SEQ-NUM> REVERSAL-DLN> SECONDARY-DT> See Instructions Below
CAF-CD> TC971/151-CD> 524 TC550DEFINER-CD> FEMA-NUM>
ULC> FREEZE-RELEASE-AMT> ABA-NUM>
TC46X-GRP-CD> TC583-DEFINER-CD>
XREF-TIN> XREF-NM-CTRL>
XREF-TIN-PRD> XREF-PLN-NUM> XREF-MFT> MISC> WI PREREF IRSERR
CORR-DT-IND> REFILE-LIEN-*IND> 2032-IND>
REMARKS: IRS Error
    
```

1. Obtain the following information:
 - Entity - SSN;
 - BOD/Function;
 - Program Name;
 - Tax Year of the TC 971 AC 524 being reversed; and

Note: The tax year must match the tax year of the TC 971 AC 524 that is being reversed.

 - Transaction date of the TC 971 AC 524 being reversed.
2. Navigate to CC FRM77
 - Sign into IDRS;
 - Enter ENMOD SSN, then press ENTER;
 - Enter CC REQ77.
 - CC FRM77 is displayed for the selected SSN.
3. Enter the TC 972 AC 524
 - Enter the TC with 972;
 - Enter TRANS-DT (enter the transaction date of the TC 971 AC 524 being reversed);
 - Enter SECONDARY-DT (enter the tax year of the TC 971 AC 524 being reversed in the MMDDYYYY format);

Note: If no SECONDARY DT is present for the TC 971 AC 524 enter "123120XX", with XX being the tax year being reversed, for secondary date field. Many 524s were input systemically (system to system) and therefore no secondary dates are present.

 - Enter MISC (BOD, Program and the reason for the reversal). Select the Reason code that reflects the reason for the reversal from the options below;

Exhibit 25.23.2-15 (Cont. 1) (11-01-2021)**TC 972 AC 524 – Reversal of TC 971 AC 524**

Note: When reversing the AC 524 because there is no date of death use “IRSERR” as the Tax Administration Source Code.

and

- Enter REMARKS (enter your remarks).

4. The following tables describe the TC 972 AC 524 Tax Administration Source Codes by BOD/Function and Program.

Note: Do not attempt to use Tax Administration Source Codes not listed for your BOD/Function.

Note: Submission Processing: will use the following for reversals as no programming is available specific to submission:

BOD: PPDS

Program: OPIP

Tax Administration Source Code: IRSERR

BOD Name	Program Name	TC 972 AC 524 Tax Administration Source Code
WI	PREREF	IRSERR
WI	AMADJ	IRSERR

TC 972 AC 524 Miscellaneous Field:

Reason	Description	Tax Administration Source Code
Taxpayer Request	The taxpayer requests the 971 be reversed.	TPRQ
Keying or Internal Error	The 971 was due to a typographical mistake or another internal mistake.	IRSERR
Internally Identified Negative Impact	The 971 is causing a negative impact on another internal process or system, and should be reversed to discontinue the negative impact. For example, a programming issue.	IRSADM
False Identity Theft Claim	RESERVED	FALSE
Other	The reason for the 971 reversal does not meet any of the above reason descriptions.	OTHER

Identity Protection and Victim Assistance - General Case Processing 25.23.2

page 147

Exhibit 25.23.2-16 (12-06-2022)

IDTVA IDRS Category Controls by Function

Employees in IDTVA-I/A will control Identity theft cases using the following category codes:

Category Code	Description	Used By
IDT1/IDS1	Taxpayer self-identified identity theft (English and Spanish). See IRM 25.23.4.4, <i>Taxpayer Inquiries Involving Identity Theft (IDT)</i> .	IDTVA-A employees working Identity Theft cases. IRM 25.23.3.2.3, <i>Self-Identified - Non-Tax-Related Identity Theft – IDT4 Overview</i> , for information on open IDT1 and IDT4 control bases receiving a TC 971 AC 123 with MISC Code: IDTVACASE.
IDT3/IDS3	Involves IRS identified identity theft. See IRM 25.23.4.4, <i>Taxpayer Inquiries Involving Identity Theft (IDT)</i> .	IDTVA-A employees working Identity Theft cases.
IDT4	Taxpayer self-identified non-tax-related identity theft. See IRM 25.23.3.2.3, <i>Self-Identified - Non-Tax-Related Identity Theft – IDT4 Overview</i> .	Primarily IDTVA IPSU, but may be systemically associated with existing tax related IDTVA controls by CII. IRM 25.23.3.2.3, <i>Self-Identified - Non-Tax-Related Identity Theft – IDT4 Overview</i> , for information on open IDT1 and IDT4 control bases receiving a TC 971 AC 123 with MISC Code: IDTVACASE.
IDT5	Responses to CP 01 Notices and/or Letter 4445C, TC 971 AC 501 Acknowledgement Notification letters. Note: Effective July 1, 2009, a CP 01, Identity Theft Claim Acknowledgement, are acknowledgement notifications of ID theft will be systemically generated in 2 to 12 cycles after input of the Transaction Code (TC) 971 Action Code (AC) 501. See IRM 25.23.3.2.4, <i>Responses to Identity Theft and IM Breach Notification Letters/Notices - IDT5</i>	IDTVA-I employees only .

Exhibit 25.23.2-16 (Cont. 1) (12-06-2022)

IDTVA IDRS Category Controls by Function

Category Code	Description	Used By
IDT6	For more information see IRM 25.23.4.6.6, <i>Credit Transcripts - IDT6/IDS6</i> .	IDTVA-A employees working credit transcripts.
IDT8/IDS8	CP 05A, (cases with prior Return Integrity & Verification Operation (RIVO) (formerly known as AMTAP) involvement) and Deceased Taxpayer cases only .	IMF AM CSRs working a tax-related issue involving identify theft. See IRM 25.23.4.8.1, <i>Streamline Identity Theft (IDT) Case Identification and Processing</i>
IDTX	Taxpayer filed Form 15227. For more information see IRM 25.23.3.2.8, <i>Application for an Identity Protection Personal Identification Number (IP PIN) Overview - Form 15227</i> .	All IDTVA Employees
GRVW	Global Review. See IRM 25.23.3.2.5, <i>Global Review - GRVW</i> .	IDTVA-I employees only .

Specialty Resolution (formerly IDTVA Compliance) employees use the Category Codes listed below to track the case status:

Category Code	Title	Definition
IDI1	Exam	Specialty Resolution - Examination cases.
IDI2	AUR	Specialty Resolution - AUR cases.
IDI3	ACSS	Specialty Resolution - ACS Support cases. (Both Domestic and International). This includes IDRS status 3.
IDI4	ASFR/CSCO	Specialty Resolution - ASFR/ASFR Recon cases. CSCO/CSCO Recon refund hold cases.
IDI5	DITA referral-Campus	Cases referred to DITA from a Specialty Resolution team for resolution.
IDI6	DITA referral - Field	Case referred to DITA from a Field operation.
IDI7		Reserved
IDI9	CSCO - TDI/TDA Programs	Specialty Resolution - CSCO - OIC, TDI and TDA.
IDII	RPM1, RPM2, RPM3 AND RPM4	Use for RPM cases